FINGERPRINT VENDOR TECHNOLOGY EVALUATION 2003

APPENDIX B

SYSTEM DESCRIPTION DOCUMENTS

The *Application to Participate in FpVTE 2003* stated:

> *3.8 Participants will be required to submit a five-page (maximum) system description document, in electronic form, on the first day of testing. (Two pages extra will be permitted for each additional system.) These documents will be included in the final FpVTE 2003 report that will be released to the public. Failure to provide this document, in its proper form, may result in not being evaluated in FpVTE 2003. This document must adequately address the following topics:*
>
> - *Overview of the evaluated system(s).*
> - *Component list for the evaluated system(s).*
> - *Detailed cost breakdown of the submitted system(s) (commercial vendors only).*
> - *Details of any modifications required to take FpVTE 2003.*

This Appendix includes those system description documents, in alphabetical order by company name.

Contents

123 ID Inc
100 North Third Street
Grand Forks, ND 58201
Ph. (701) 780-9882
Fax. (701) 775-3909
email: info@123id.us

FpVTE 2003 System Description
LST Level

Overview

The underlying infrastructure and product conducting the biometric search for the LST level fpVTE2003 competition is the Biometric System Service (BSS) from 123ID, Inc.

The BSS is a biometric search cluster system designed to offer scalability and hardware independence.

Software components

a) The BSS cluster system

The software component of BSS automatically manages, distributes and redirects, incoming search loads among its multiple search nodes (CPUs) independent of the application requesting the search service.
The components building the BSS system are:

- Communication Service -
  Receives application (client) requests and communicates with Resolution service
- Administration Service -
  Configures Nodes and search balance. Defines I/O of BSS system
- Resolution Service -
  Carries out system configuration.
- Node service -
  Carries out the search task assigned to each node.

b) The Code Vector (CVT) matching technology

CVT defines and analyzes a pattern (initially from fingerprints but potentially expandable to Iris, face or palm) based on its vector behavior, morphology and minutia distribution.

CVT rates the similarity of two fingerprints based on a score ranging from 0 to 1,073,741,824, allowing CVT great discrimination capability sufficient for 1-many applications.
Traditionally the cutoff score for a positive match is set based on the fingerprint data capture modality (partial versus full print), and the type of match (1-1 or 1-n). For the LST fingerprint database, only full prints (no partial or latent) prints are expected and a 1-Many scenario is assumed.

The acceptance score for a positive identification is set at 420,000 based on the LST sample database. Technically, the score cut off should be set at a range based on a full analysis. Since we were unable to analyze the full LST database, the current CVT configuration is only based on the LST Sample database.

CVT is configured for a FAR equal to zero based on the LST sample database; Additionally, the separation between false accept and false reject similarity events can be appreciated by the range of score separation displayed by CVT. The appearance of FAR events on the complete database are possible since CVT for the FpVTE2003 competition was configured based on a small sample data; however, by shifting the positive matching score upwards, a desired FAR can be achieved.

CVT is conversely configured for the smallest FRR possible. The following limitation are assumed and expected to produce False Rejections or FTE:

1. Matching score < 420,000 (non-normalized)
2. Matrix size of 150 x150 pixels or less
3. Fingerprint images coming from different scanner sources with aspect ratio incorrectly applied producing an inconsistent special mapping. See document “Inconsistencies in aspect ratio normalization from different fingerprint capture sources.”
4. Fingerprints excluded due to poor quality as indicated by the TQI index from the BX quality control are used to represent the FTE Threshold.

The rotation permitted based on the ranges described by NIST is 60 degrees from the orientation of the target fingerprint.

c) The Biometric Exchange (BX) quality assessment product

The quality of a fingerprint image is assessed by multiple indexes, which are combined to ultimately derive the overall quality of the image as well as local quality assessment and reliability.
The BX quality control generates a total quality index (TQI) used to accept/reject a fingerprint and even to reject a print for enrollment (FTE). The FTE cutoff for the NIST FpVTE2003 competition is set to 65%.

The TQI is composed of six different and yet complementary indexes that can be further described upon request. An application creating the full set of indexes and their respective quality control image masks is also available upon request.

The BX quality assessment and the BX product in general are independent of the CVT technology.

c) The Virtual Print Signature Technology (VPSignature)

Virtual Print Signature (VPSignature™) is a numeric indexing technology created by 123ID to search very large scale databases. VPSignature™ numerically describes the morphology of a fingerprint pattern. It was designed to divide a large database based on the numeric representation of the fingerprint morphology.

Only those subject Ids that created discrepancies in the Vpsignature match among different fingerprints of the same subject were grouped as potentail false accepts. However, all fingerprints of a subject that passed the quality standard enforced were processed with the VPSignature technology.

The potential false accepts were processed by a second pass with the exhaustive CVT matching technology described above.

Hardware components

The BSS is composed of 36 Search nodes and an administrator. The search nodes are managed by an administration node via standard network communication.

Detailed Cost Breakdown

The BSS solution is packaged along with an Alias Elimination Service – AFE product from 123ID, Inc.

The AFE software is priced as a service per user enrolled in the database for unique identity management. The price per user template is $12. Special discounts apply to government agencies.

The cost of the hardware used for the FpVTE competition with the following components is $98,000:

1. Administrator Node
   - CCSI Clusteron Athlon Head Node, MP 2600 CPU, 2 GB RAM, 130 GBHD

2. Search Nodes
   - CCSI Clusteron UltraCool Athlon Nodes MP 2600 CPU CPU, 1GB RAM, 30 GBHD
3. UPS backup for Rack system
4. Ethernet HUB for 40 points

123ID does not sell hardware, the cost above is the cost to 123ID.

Modifications required for the FpVTE event

The basic BSS system has undergone the following minor changes for the FpVTE competition:

1. Adjustment of the Input to accept WSQ (.an) files
2. Adjustment of the Output to create the sim files
3. Adjustment of the matching Code Vector Technology (CVT) to the 500 pixels per inch resolution assumed by NIST.
4. Creation of a FAR and FRR graphical evaluation module based on the nomenclature defined by NIST for the FPVTE.

123 ID Inc
100 North Third Street
Grand Forks, ND 58201
Ph. (701) 780-9382
Fax. (701) 775-3909
email: info@123id.us

FpVTE 2003 System Description
MST Level – 2nd run
(123IDIM2)

Overview

The underlying infrastructure and product conducting the biometric search for the MST level fpVTE2003 competition is the Biometric System Service (BSS) from 123ID, Inc.

The BSS is a biometric search cluster system designed to offer scalability and hardware independence.

Software components

a) The BSS cluster manager

The software component of BSS automatically manages, distributes and redirects, incoming search loads among its multiple search nodes (CPUs) independent of the application requesting the search service.
The components building the BSS system are:

- Communication Service -
  Receives application (client) requests and communicates with Resolution service
- Administration Service -
  Configures Nodes and search balance. Defines I/O of BSS system
- Resolution Service -
  Carries out system configuration.
- Node service -
  Carries out the search task assigned to each node.

b) The Code Vector (CVT) matching technology

CVT defines and analyzes a pattern (initially from fingerprints but potentially expandable to Iris, face or palm) based on its vector behavior, morphology and minutia distribution.

CVT rates the similarity of two fingerprints based on a score ranging from 0 to 1,073,741,824, allowing CVT great discrimination capability sufficient for 1-many applications.
Traditionally the cutoff score for a positive match is set based on the fingerprint data capture modality (partial versus full print), and the type of match (1-1 or 1-n). For the MST fingerprint database, only full prints (no partial or latent) prints are expected and a 1-Many scenario is assumed.

The acceptance score for a positive identification is set at 420,000 based on the MST sample database. Technically, the score cut off should be set at a range based on a full analysis. Since we were unable to analyze the full MST database, the current CVT configuration is only based on the MST Sample database.

CVT is configured for a FAR equal to zero based on the MST sample database; Additionally, the separation between false accept and false reject similarity events can be appreciated by the range of score separation displayed by CVT. The appearance of FAR events on the complete database are possible since CVT for the FpVTE2003 competition was configured based on a small sample data; however, by shifting the positive matching score upwards, a desired FAR can be achieved.

CVT is conversely configured for the smallest FRR possible. The following limitation are assumed and expected to produce False Rejections or FTE:

1. Matching score < 420,000 (non-normalized)
2. Matrix size of 150 x150 pixels or less
3. Fingerprint images coming from different scanner sources with aspect ratio incorrectly applied producing an inconsistent special mapping. See document “Inconsistencies in aspect ratio normalization from different fingerprint capture sources.”
4. Fingerprints excluded due to poor quality as indicated by the TQI index from the BX quality control are used to represent the FTE Threshold.

The rotation permitted based on the ranges described by NIST is 60 degrees from the orientation of the target fingerprint.

c) The Biometric Exchange (BX) quality assessment product

The quality of a fingerprint image is assessed by multiple indexes, which are combined to ultimately derive the overall quality of the image as well as local quality assessment and reliability.
The BX quality control generates a total quality index (TQI) used to accept/reject a fingerprint and even to reject a print for enrollment (FTE). The FTE cutoff for the NIST FpVTE2003 competition is set to 45%.

The TQI is composed of six different and yet complementary indexes that can be further described upon request. An application creating the full set of indexes and their respective quality control image masks is also available upon request.

The BX quality assessment and the BX product in general are independent of the CVT technology.

Hardware components

The hardware component of BSS is composed of 16 Search nodes and an administrator. The search nodes are managed by an administration node via standard network communication.

Detailed Cost Breakdown

The BSS solution is packaged along with an Alias Elimination Service – AFE product from 123ID, Inc.

AFE is priced per user enrolled in the database for unique identity management. The price per user template is $12. Special discounts applied to government agencies.

The cost of the hardware used for the FpVTE competition with the following components is $55,000:

1. Administrator Node
   - HP a330n 1.8 GHz CPU, 1GBRAM

2. Search Nodes
   - CCSI Clusteron UltraCool Athlon Nodes MP 2600 CPU CPU, 1GB RAM, 30 GBHD
3. UPS backup for Rack system
4. Ethernet HUB for 40 points

123ID does not sell hardware, the cost above is the cost to 123ID.

Modifications required for the FpVTE event

The basic BSS system has undergone the following minor changes for the FpVTE competition:

1. Adjustment of the Input to accept WSQ (.an) files
2. Adjustment of the Output to create the sim files
3. Adjustment of the matching Code Vector Technology (CVT) to the 500 pixels per inch resolution assumed by NIST.
4. Creation of a FAR and FRR graphical evaluation module based on the nomenclature defined by NIST for the FPVTE.

Antheus Technology, Inc.

System Description

System Overview

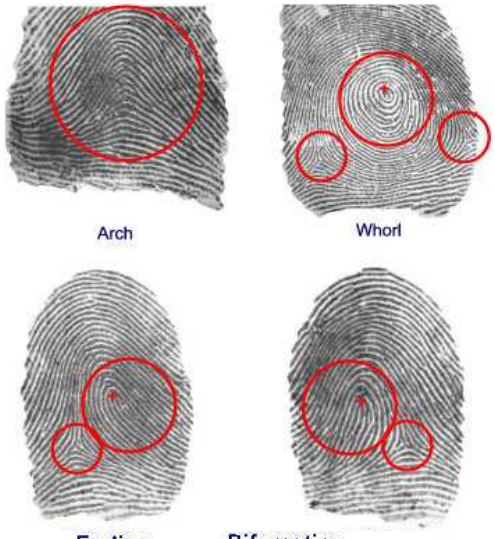
Antheus Technology Inc. is pleased to participate in the FpVTE 2003. The opportunity to test our accurate technology using real life fingerprints is a challenge that we undertake with pride and high expectations. Antheus is a premier developer of fingerprint identification software. Agora is a highly accurate fingerprint identification software that extracts minutiae points and accurately matches thousands of fingerprints at sub-second speed. Thanks to its precise matching algorithms Agora is a world class Automatic Fingerprint Identification System (AFIS) for civil identification and criminal investigation.

Overview of Fingerprints

The fingerprints of different people and even from the same person differ according to two criteria. The first one is related to the *group* the finger belongs to, and the second criterion is related to the *minutia points*. The group criterion represents a macro vision of the fingerprints, defined by the patterns followed by the finger ridges. Based on those patterns a fingerprint is classified and placed in a group as an Arch, a Whorl, a Left Loop, a Right Loop or No Classification. Agora's fingerprint search engine optionally first attempts to find the person in the corresponding group, and within the group it conducts a second search based on minutiae points. A cold search based only on minutiae poits is also possible.

The Groups

Arch: The ridges form on one side and tend to go through to the other side of the finger.
Whorl: The ridges tend to present a concentric pattern, spiraled, ovoid or sinusoid, all on the center of the finger image.
Right Loops: The ridges flow from the right of the observer, curve at the center of the fingerprint and tend to go back to the same side.
Left Loops: The ridges flow from the left of the observer, curve at the center of the fingerprint and tend to go back to the same side.



Cores and Deltas

The finger images of the group classifications Whorl and Loops (Right and Left) present two additional characteristics to sharpen the pattern classification even more, and help in the process of comparison. The Core of a fingerprint represents its "center of gravity". It is located on the upper part of the most internal curved ridge in the whorl. In the Left and Right Loops is in the top of the most internal ridge that loops. In the figure above is indicated with a "+" sign. The homogeneity of the ridges in the Arches normally impedes the automatic positioning of the Core, but this does not affect the accuracy of Agora.

The Deltas are the divergence points where the ridges tend to wrap around the center of the finger. The Whorls usually have two Deltas; the Right Loops have a Delta on the left of the observer, and the Left Loops to the right of the observer. Agora automatically determines the Groups, Cores, Deltas and Minutiae Points if they are all or partially available for each particular fingerprint, and with this information it generates a finger image template, or Code that is used for searching and matching.

Antheus Technology, Inc.
22241 Larkspur Trail, Boca Raton, FL 33433, USA
tel +1 561 417 3876, eFax +1 423 502 6637
email: info@antheustechnology.com ; web: www.antheustechnology.com

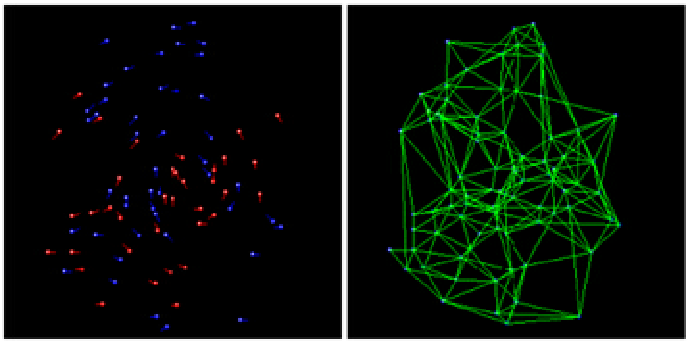
Antheus Technology, Inc.

Agora Analysis

The generation of templates used in searching and the matching of a fingerprint against a database, is the result of a series of software routines to extract relevant features. Following are the sequential steps used by Agora: Image Crop, Directions, Binarization, Thinning, and Minutiae Extraction

Template Generation

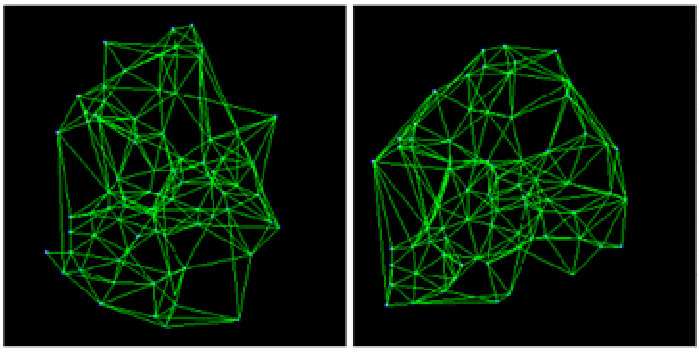
The Minutiae Points extracted in the Analysis phase are the foundation for the search and match of fingerprints. A template represents a planar distribution of the minutiae. The template establishes a relationship taking into account the distribution of minutiae on a fingerprint. The template contains the data regarding the distribution, type, orientation and cross-relationships between the minutiae. The template associated with the fingerprint image is stored in the database.



Minutiae | Template Code

Template Code for different images of the same fingerprint.

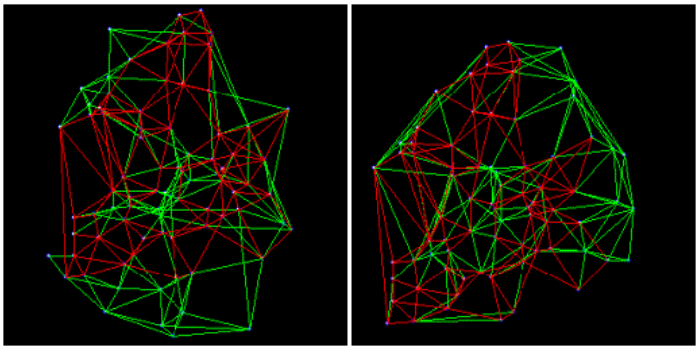
The Search / Match operation is a restricted isomorphism of the Search template and the Candidate template. Changes in pressure at capture, rotations, disturbances on the ridges due to cuts or scars, are impediments to a total isomorphism. Two fingerprints from the same person result in Template Codes that are visually different. The Matching problem is to determine "how much" of a Template Code is included in the other one. The templates above correspond to two images captured from the same finger, within a two month interval. The complete difference between the two is an illusion. The function of Agora's matching algorithms is to find the resemblance.



Template Code 1 | Template Code 2

The Matching of Searched and Candidate Templates

The matching of Searched and Candidate fingerprints is a comparison of two templates. The minutiae that correspond to both templates are highlighted. The total of correspondences is used to determine a degree of similarity between the templates, and this degree or ratio indicates whether the templates come from same finger.



Templates obtained from two images of the same finger with common sub-templates highlighted

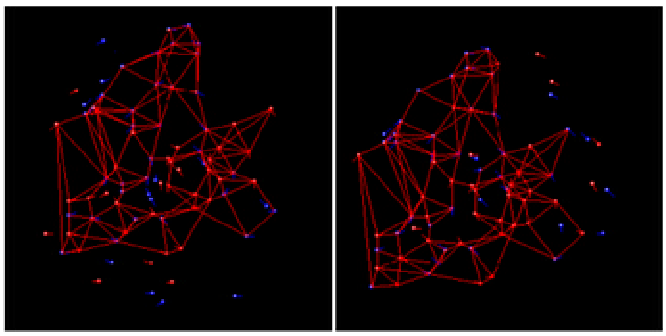
Antheus Technology, Inc.
22241 Larkspur Trail, Boca Raton, FL 33433, USA
tel +1 561 417 3876, eFax +1 423 502 6637
email: info@antheustechnology.com ; web: www.antheustechnology.com

Antheus Technology, Inc.

The Mapping

The result of the Matching is a new Template contained in both compared templates. In this new template named Mapping the minutiae point and the lines that are in both templates are highlighted.

The minutiae that can't be mapped are not counted to determine the similarity. The figure above shows minutiae that have not been mapped for both finger images. The presence or absence of minutiae in one or the other fingerprint is an indication of the difference in pressure, rotation or translation of the finger in the different captured images.



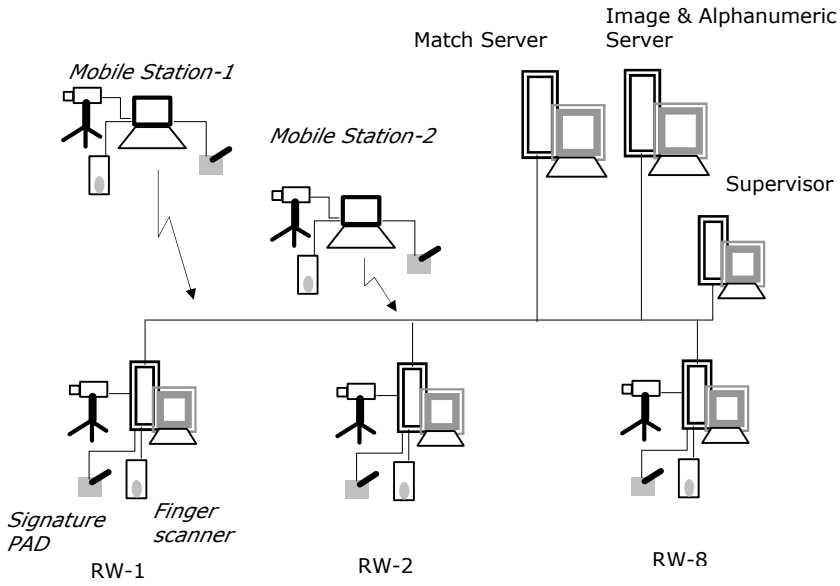
View of the Mapping between both fingerprints, and non-paired minutiae

Agora Architecture

There are three distinct elements of Agora application architecture:

1. The Client Station used for enrollment, verification and / or identification. This is the user interface.
2. The Database Server that contains all identities' records, including images, demographic information and biometric templates.
3. The MatchServer that performs the fingerprint comparisons.

The Client Station, Database Server and MatchServer may be configured in different ways depending on the project requirements. Of these three elements Agora supplies the biometric software tools for the Client Station and the MatchServer application software.



Registration

The systems integrator adds:

1. The Database Server including hardware, base software and database management system software.
2. The Client Station, including hardware, base software, application, networking software, and peripherals.
3. Integration to the Search / Match application software.- Integration to the Agora biometric software tools for the Client Station.
4. Project Implementation.

Antheus Technology, Inc.
22241 Larkspur Trail, Boca Raton, FL 33433, USA
tel +1 561 417 3876, eFax +1 423 502 6637
email: info@antheustechnology.com ; web: www.antheustechnology.com

Antheus Technology, Inc.

How to Order

1 Order the Agora Software Developers Kit with WSQ (ANASNW). If all you need is WSQ compression / decompression, then order the Agora WSQ Software Developers Kit (ANASW)

2 Decide how many workstations will need Agora FingerClient (ANAR1), the extract and match Licenses, and how many will need Agora WsqClient (ANARW), the WSQ compression / decompression licenses. If you need to search against a database using fingerprints then go to step 3, otherwise stop right here.

3 Determine the number of persons in the database. Then choose your Agora MatchServer License (ANAM1, 2, 3)

Product	Product Description
ANASNW	Agora Software Developers Kit 2.5 with WSQ, 1-1 verification and MatchServer for up to 1,000 identities using 1 to 10 fingers each identity; includes components for flat or rolled* finger image capture using Cross Match USB scanners or Video for Windows; Analysis and Fingerprint Code Generation and 1-1 Matching (extract and match); Display of Minutiae Points and Graphics; WSQ** for fast compression and decompression of grayscale fingerprint images. Includes DLLs, ActiveX Control or COM-DLL; several sample applications with source code (Visual C++/Visual Basic); Documentation; Agora Demonstration Software Application; Agora WSQ Demonstration Software Application; Runtime License for Windows 98/Win Me/NT/2000. *Rolled Print capture available only for Cross Match V300 RS-170 and Integral FlashBus MV Series frame grabber. **WSQ certification number 45100 by the US Federal Bureau of Investigation (FBI).
ANAR1	Agora FingerClient, extract and match for 1-1 verification runtime license for the client for Windows 98/Win Me/NT/2000/XP; includes components for Analysis, Fingerprint Code Generation that extracts minutiae file usable by the Agora MatchServer, and 1-1 Matching (extract and match); Capture of flat or rolled* finger images using Cross Match USB scanners, Identix DFR200 or Video for Windows; Photo Capture with Video for Windows driver; Display of minutiae point and graphics. *Rolled Print capture available only for Cross Match V300 RS-170 and Integral FlashBus MV Series frame grabber
ANASW	Agora WSQ Software Developers Kit 2.5 - WSQ for fast Compression and Decompression of grayscale fingerprint images. Includes DLLs, ActiveX Control or COM-DLL for WSQ Compression and Decompression; components to capture flat or rolled* fingerprints using Video for Window drive, Cross Match USB Sensor or Identix DFR200, Sample App in source code (Visual C++/Visual Basic); documentation; includes one Runtime License and Agora WSQ Demonstration Software Application; for Windows 9x/Me/2000. US Federal Bureau of Investigation (FBI) certification number 45100. *Rolled Print capture available only for Cross Match V300 RS-170 and Integral FlashBus MV Series frame grabber
ANARW	Agora WsqClient for WSQ compression and decompression of grayscale fingerprint images runtime license for Windows 98/Win Me/NT/2000/XP. Includes DLLs, ActiveX Control or COM-DLL for WSQ compression and decompression; components to capture flat or rolled* fingerprints using Video for Windows driver, Crossmatch USB Sensor or Identix DFR200; for Windows 9x/Me/2000. US Federal Bureau of Investigation (FBI) certification number 45100. *Rolled Print capture available only for Cross Match V300 RS-170 and Integral FlashBus MV Series frame grabber
ANAM1	Agora MatchServer ten fingerprints from 1 to 1,000 identities Search / Match Server Runtime License for Windows 95/98/NT/2000/XP
ANAM2	Agora MatchServer ten fingerprints from 1001 to 10,000 identities Search / Match Server Runtime License for Windows 98/NT/2000/XP
ANAM3	Agora MatchServer ten fingerprints 10,001 to 50,000 identities Search / Match Server Runtime License for Windows NT/2000/XP/2003 Server
ANAMC	Agora MatchServer Configurable ten fingerprints from 50,000 to N identities Search / Match Server Runtime License for Windows NT/2000/XP/2003 Server. Ask how to complete survey and request quote

Antheus Technology, Inc.
22241 Larkspur Trail, Boca Raton, FL 33433, USA
tel +1 561 417 3876, eFax +1 423 502 6637
email: info@antheustechnology.com ; web: www.antheustechnology.com

Antheus Technology, Inc.

Component list forthe FpVTE2003

Description	Cost
Software	
Windows 2000 Server with SP4	$800
Custom developed FpVTE.exe application statically linked to standard and custom libraries as listed in Configuration Management, including WSQ compression / decompression version 2.5 developed by Antheus and certified in August 1st 2001 by the FBI with software implementation value (sf), within the frame header of the compressed image recorded as 45100.	$895
Hardware	
Dell PowerEdge 2600, dual Pentium 4 at 2.8 Ghz, 1GB RAM, 1 x 36GB 10,000 rpm SCSI disks, keyboard and mouse	$2,800
NEC AccuSync LCD5V monitor	$280
Total	**$4,775**

Modifications for the FpVTE 2003

We developed a custom made application to conduct the MST and LST automatically with minimum operator interface, that uses Antheus' standard libraries and some custom made libraries specific for the test. This application uses one of our most accurate fingerprint matching algorithms that is implemented worldwide in accurate software based, standard compliant AFIS systems. It can complete the LST in three weeks with one $2,500 dual-processor Windows 2000 server. Other than that no other modifications were introduced to our technology.

Antheus Technology, Inc.
22241 Larkspur Trail, Boca Raton, FL 33433, USA
tel +1 561 417 3876, eFax +1 423 502 6637
email: info@antheustechnology.com ; web: www.antheustechnology.com

The Systems used by Av@lon Systems in the FpVTE 2003

1 SYSTEMS OVERVIEW

Av@lon Systems participated in the FpVTE 2003 with two different systems, one for the Medium Scale Test (MST) the other for the Large Scale Test (LST). The two systems differed not only in the hardware but also in the software modules and matching algorithms they used to perform the respective test.

The software solution **ULTRAMATCH AFIS** that was used to perform both tests consists of the following modules.

ULTRAMATCH AFIS is a fingerprint specific implementation of UltraMatch and consists of the software modules as outline in the drawing above. **ULTRAMATCH** is a technology that uses an absolutely new matching technology based on a neural network with unique algorithms. UltraMatch is able to work with BIR templates from Iris scan to face recognition or any other biometric templates and to use the same matcher software to match all these various template formats.

ULTRAMATCH AFIS is platform independent and can be implemented from a single workstation via workstation clusters to a proprietary computer board based solution, depending on the demand of matches per second.

1.1.1 Features & Benefits of UltraMatch AFIS

Extreme fast Data Access
UltraMatch AFIS is based on a massive parallel processing database. The neural net is reacting with stimuli pattern to the process impulse. These stimuli are reacting simultaneously like an avalanche. UltraMatch AFIS is an extremely fastest matcher in the market.

Easily scalable Database
UltraMatch AFIS contains a smart solution for clustering servers in order to setup large server farms to process millions of fingerprint templates or other data records.

Self organized Neural Data Storage
For the first time in computing, UltraMatch AFIS is using a neural net to store data in form of structure. The advantages of storing data directly in a neural net are almost unlimited regarding, i.e. speed and quality of data processing.

Flexible in Data Storage Structure
Another milestone in software architecture is the fact that the internal organization of the database is flexible in accepting any kind of data structure as import. Therefore data migration and data base merging are additional advantages of Stellaris.

Rollback and 100% Safety against Loss of Data
UltraMatch AFIS includes the full functionality of rollback and replication of the data base and data sets. The UltraMatch database is the fastest and safest database concept available.

Generic Interface for API's and 3rd party DB's
GIP, the interface protocol, can communicate with any other data base. Just instruct UltraMatch about the data structure of the other database, UltraMatch AFIS can thereafter automatically start the communication between different databases and different protocols.

Worldwide New generation of Generic Algorithms
UltraMatch AFIS is based on the mathematical theory of "the generic algorithm" of Manfred Hoffleisch. UltraMatch AFIS is using the stored structure of the many fingerprint templates in the neural net to compare and analyze spontaneously with the reference pattern.

Spontaneous mode of Operation
Due to the fact that that stored fingerprint templates are stored directly as structure in a neural net, there is no need for indexing or classification of the data. This enables UltraMatch AFIS to spontaneous operations right after importing the data.

Extremely fast Data Matching
The time for a match is 0.000004 sec using a P4 3.0GHz processor and 333MHz RAM workstation. Thus we are able to match i.e.1 NIST fingerprint template against 200.000 fingerprints in 0.8 seconds.

Alphanumeric, semantic & associative Data Mining

The neural data process offers one more significant attribute, the semantic and associative alphanumeric data mining (not used in UltraMatch AFIS). The generic API can answer context orientated and instantly to any data mining question.

Pattern comparison

UltraMatch AFIS offers a generic and precise pattern matching because it combines the generic algorithm with the self organized neural data storage.

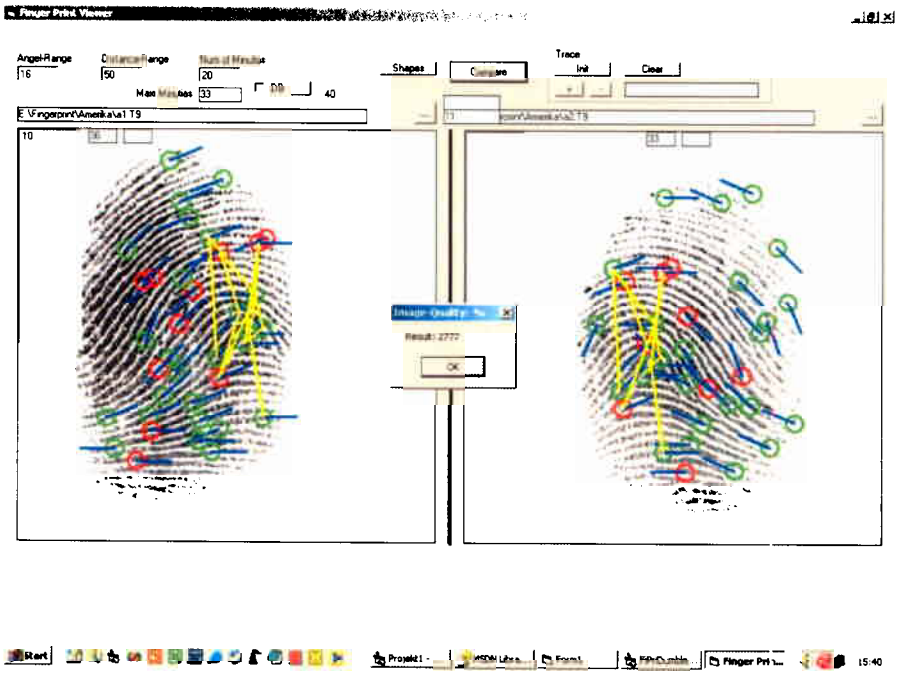
The following chapter describes the main modules of UltraMatch AFIS as they are outlined in the systems overview.

1.2 Stellaris AI Database

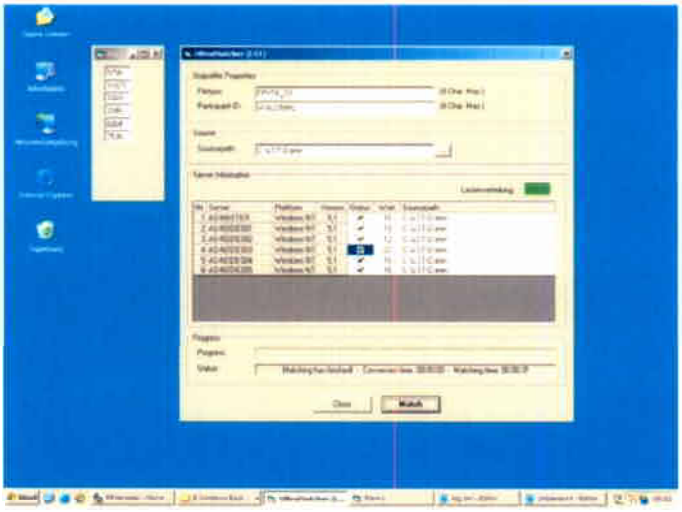
UltraMatch AFIS is storing fingerprints in form of a neural net called Stellaris. This neural net is based on a breathtaking new concept, founded by Manfred Hoffleisch, Head of R&D of semantic system ag. This neural net represents an extreme fast data processing and data storing capability. The Stellaris AI database is absolute self organizing and needs no supervision or administrative effort. Using the Stellaris AI database enables a constant match time of 0.0005 seconds per fingerprint template.

1.3 UltraMatch Algorithms

The new concept of Manfred Hoffleisch's neural net is based on an intrinsic, self organized algorithm. One of the capabilities of this algorithm is the generic pattern recognition. UltraMatch is able to recognize and compare any biometrics template with a few adaptations to its algorithm. In the event of fingerprints, this algorithm is used to recognize fingerprint templates extremely accurate and precise.



1.4 UM Supervisor



The UM Supervisor will organize the matching process and workflow. Depending on the size of the Stellaris AI database and the matches to be performed, UltraMatch will run on a single PC or on a cluster of PCs with scalable load balancing or on proprietary computer boards.
The UM Supervisor distributes fingerprint templates throughout the configurations, it coordinates fingerprint comparisons amongst the entire distributed Stellaris AI database and it compiles comparison results of the distributed database. In general any platform and operating system can be used.

1.5 UM AFIS Console

The UM AFIS Console from Av@lon Systems providers the GUI, administration and management of the entire UltraMatch AFIS as a hardware and software solution. It consists of at least the following modules:

- **Monitor**; monitors the performance of UltraMatch in batch mode. It provides statistics and performance parameters like hit list, thresholds etc.
- **Match**; performs 1:1 matches in an online mode and performs 1:N matches in batch mode with certain setup parameters.
- **Setup**; enables the user to connect to a certain UltraMatch AFIS database and defines various other parameters like path names, thresholds, license keys, etc.
- **Admin**; User administration, bio-logon, add, change, delete fingerprint templates and its wsq files; backup of Stellaris databases.
- **Reports**; prints various reports and statistics; focusing on hitlists, match performance exceptions, etc.
- **Investigate**; Investigating in detail fingerprint images by various means to support human based decisions.

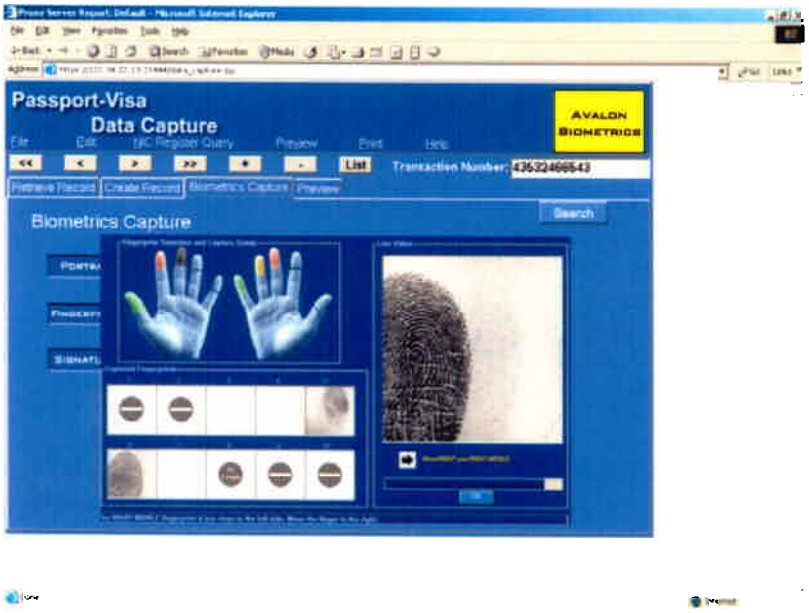
1.6 Agora NIST Encoder

The Agora NIST Encoder, from Antheus Technology, is an extract and match for 1-1 verification runtime license for the client for Windows 98/Win Me/NT/2000/XP; includes components for Analysis, Fingerprint Code Generation that extracts minutiae file usable by UltraMatch. It captures flat or rolled* finger images using Cross Match USB scanners, Identix DFR200 or Video for Windows; Photo Capture with Video for Windows driver; Display of minutiae point and graphics. *Rolled Print capture is available only for Cross Match V300 RS-170 and Integral FlashBus MV Series frame grabber.

1.7 Agora WSQ Compression

Agora WSQ Compression is for WSQ compression and decompression of grayscale fingerprint images runtime license for Windows 98/Win Me/NT/2000/XP. It includes DLLs, ActiveX Control or COM-DLL for WSQ compression and decompression; components to capture flat or rolled* fingerprints using Video for Windows driver, Crossmatch USB Sensor or Identix DFR200; for Windows 9x/Me/2000. US Federal Bureau of Investigation (FBI) certification number 45100. *Rolled Print capture available only for Cross Match V300 RS-170 and Integral FlashBus MV Series frame grabber.

1.8 UM AFIS Live Enroll



An ActiveX control, called from a client application or a web page, performs the capture of the requested number of fingers, performs quality assurance on each finger and the capture process.

The images will be wsq compressed, a NIST type 4 record is created and the ActiveX control submits the data to the workflow application.

2 COMPONENT LIST

2.1 Component List for MST

2.1.1 Hardware

Workstation:	1 DELL Inspiron 5150 notebook
Processor:	1 P4 with 3.0 GHz
Main memory:	1 GByte
Misc.:	Hard disk, CD Drive, off the shelf configuration

2.1.2 Software

Operating System:	Windows XP professional
Fingerprint Analyzer:	Antheus Type 9 analysis (extracts, or encodes)
Compression Software:	Agora WSQ compression / decompression
Fingerprint Encoder:	Agora Analysis (extracts, or encodes)
Database:	Stellaris AI
Match Algorithm:	UltraMatch
Workflow:	UltraMatch Manager, MD5 Algorithm

2.2 Component List for LST

2.2.1 Hardware

Workstation:	4 x DELL Dimension 2300
Processor:	4 x Intel Celeron 1.7 Ghz
Main memory:	4 x1 GByte
Misc.:	4 x Hard disk, CD Drive, monitor, keyboard, mouse
Workstation:	2 x HP Pavillion 514N
Processor:	2 x Intel P4 2.2 Ghz
Main memory:	2 x 1 GByte
Misc.:	2 x Hard disk, CD Drive, monitor, keyboard, mouse
LAN:	1 x 8 port Netgear switch, 6 patch cable

2.2.2 Software

Operating System:	Windows XP professional
Fingerprint Analyzer:	Antheus Type 9 analysis (extracts, or encodes)
Compression Software:	Agora WSQ compression / decompression
Fingerprint Encoder:	Agora Analysis (extracts, or encodes)
Database:	Stellaris AI
Match Algorithm:	UltraMatch
Workflow:	UltraMatch Manager, MD5 Algorithm

3 DETAILED COST BREAKDOWN

3.1 Cost Breakdown MST

Item	Vendor	Price in USD
Inspiron 5150 Notebook	DELL	2328
Type 9 analysis	Antheus	195
Agora WSQ compression / decompression	Antheus	395
Agora Analysis (extracts, or encodes)	semantic system	195
Stellaris AI	semantic system	1600
UltraMatch	semantic system	800
UltraMatch Manager, MD5 Algorithm	semantic system	600

3.2 Cost Breakdown LST

Item	Vendor	Price in USD
4 x DELL Dimension 2300	DELL	4 x 799
2 x HP Pavillion 514N	HP	2 x 749
1 x 8 port switch	NetGear	112
Type 9 analysis	Antheus	195
Agora WSQ compression / decompression	Antheus	395
Agora Analysis (extracts, or encodes)	semantic system	195
Stellaris AI	semantic system	8000
UltraMatch	semantic system	4000
UltraMatch Manager, MD5 Algorithm	semantic system	3000

4 MODIFICATIONS FOR FPVTE

The only modifications made are regarding the specific workflow and data formats of the FpVTE 2003 test. The UltraMatch AFIS runs in a standard configuration.

BioLink
Advanced Biometric Solutions

11360 Interchange Circle North
Miramar, Florida 33025 USA
Phone: +1 954 450-7061
Toll Free: (800) 611-1555
Fax: +1 954-450-7062
www.biolinkusa.com

System Description

Document

For The

Fingerprint Vendor Technology Evaluation

Large-Scale Test

Submitted To

National Institute of Standards and Technology

By

BioLink Technologies International

Contact:
John C. Schmitt, Ph.D
VP – ID Systems
11360 Interchange C., N
Miramar, FL 33025
(321) 452-9390

BioLink's FpVTE Large-Scale Test Configuration Overview and Component List

BioLink's Authenteon-based FpVTE LST system submitted consists of two main subsystems:

A) A Control Front End (CFE) which interfaces to the outside world (I/O to the System) as well to the Search Engine (Back End). It's major functions are to accept input imagery, decompress and extract minutia from these, manage match operations per XML instructions, submit fingerprints to the Search Engine, accept results of match operations, and format match score results for output. All of the semantics of the application are contained in the CFE and are developed and implemented via a sophisticated BioLink SDK known as the Authenteon Toolkit (ATK). Components of the CFE are:

   Platform – BioLink-assembled PC with the following characteristics: Pentium-IV Processor, 2.6 GHz, 512 MB RAM, 60 GB hard disk. There are two of these platforms, one for the CFE itself and one for the computer to host the SQL Server database.

   Software – OS is Windows Server 2003. The Authenteon Connection Toolkit (ATK)* version 1.2.24.2 provides the control functionality. SQL Server 2000 (Service Pack 3) from Microsoft provides the RDBMS. A custom Windows application for FpVTE known as FpVTE Application* version 66 supports the unique requirements related to data input, reporting of output matrices, etc. Aware Corporation's WSQ decompression software version 2.5 is used to decompress ANSI/NIST-compliant records and images.

B) A Search Engine consisting of one or more single-board ("blade") computers each of which maintains 1/Bth of the fingerprint minutia data base (where "B" is the number of blades). The Search Engine only responds to commands from the CFE and knows nothing of the semantics of the application whether it is an elections system, a driver license issuance system, or an FpVTE.

   Platform – 24-each RLX Corporation model 1200i processing blades, with main processor Pentium-III, 1.3 GHz, 512 MB RAM. These are housed 12 to a chassis in (2) RLX model 300ex chassis.

   Software – OS is Red Hat Linux 7.2 with RLX version 2.4.9-3 kernal and other RLX-specific drivers. Main fingerprint matching software is BioLink Authenteon Cluster Array version 1.2.0.54.

Cost Breakdown for BioLink Components for FpVTE LST System

- Authenteon Search Engine Blade (hardware from RLX) including Authenteon Cluster Array software, $11,250.
- RLX chassis supporting up to 12 Search Engine Blades, $2,800.
- Authenteon Connection Toolkit (ATK) SDK $995.
- SQL Server, Windows Server 2003, see Microsoft Corporation
- ANSI/NIST decompression software, see Aware Corporation

* Authenteon Connection Toolkit and FpVTE Application will be made available to any authorized Government organization which wishes to replicate our FpVTE configuration.

Modifications Required to take FpVTE

Only as described above to apply core commercial technology offered by BioLink in the custom application configuration specified by NIST for the FpVTE. The specifics of the LST subtest scripting, as well as many of the data input and output requirements, are unique to FpVTE. This custom configuration is implemented via our FpVTE Application version 66 which we offer to make available to authorized Government organizations which wish to replicate our FpVTE configuration.

BioLink
Advanced Biometric Solutions

11360 Interchange Circle North
Miramar, Florida 33025 USA
Phone: +1 954 450-7061
Toll Free: (800) 611-1555
Fax: +1 954-450-7062
www.biolinkusa.com

System Description

Document

For The

Fingerprint Vendor Technology Evaluation

Medium-Scale Test

Submitted To

National Institute of Standards and Technology

By

BioLink Technologies International

Contact:
John C. Schmitt, Ph.D
VP – ID Systems
11360 Interchange C., N
Miramar, FL 33025
(321) 452-9390

BioLink's FpVTE Medium-Scale Test System Overview and Component List

BioLink's Authenteon-based FpVTE MST system submitted is extremely simple from a components standpoint and consists of BioLink's custom FpVTE Application version 66 running in an industry-standard PC with COTS operating system.

Platform – BioLink-assembled PC with the following characteristics: Pentium-IV Processor, 2.6 GHz, 512 MB RAM, 60 GB hard disk, CD read/write drive.

Operating System – Microsoft Windows Server 2003.

FpVTE Application – this application (BioLink's version number 66) supports the unique requirements generated for the FpVTE. It's core image processing and minutia extraction and matching technologies are exactly the same as for all other BioLink Authenteon products, but it constitutes a unique configuration not offered commercially by BioLink. Rather, BioLink's one-to-many products are more commonly offered in the blade configuration Search Engine submitted for the LST. There are very likely to be found no commercial requirements for MST's basic functionality, which is to take in 10,000 prints and cross-match them and output a 100 million-cell matrix of similarity scores for later research and analysis purposes.

Nonetheless, FPVTE consists of the following functionality. It accepts the fingerprint database in accordance with NIST's specifications. It opens the ANSI/NIST-compliant records and decompresses the images using Aware Corporation's WSQ decompression software version 2.5. It extracts the 10,000 minutia templates from the images. It then calls a DLL which systematically ("for i = 1 to 10,000; for j = 1 to 10,000") runs a match score algorithm computing a similarity score for each of these 100 million pairs of templates. It then formats the similarity matrix for output in accordance with NIST's specification and writes all required data to a CD.

Cost Breakdown for BioLink Components for FpVTE MST System

For reasons as stated above, BioLink's FpVTE MST configuration is not currently offered as a commercial product.

Modifications Required to take FpVTE

Only as described above to apply core commercial technology offered by BioLink in the custom application configuration specified by NIST for the FpVTE. The specifics of the MST crossmatch task, as well as many of the data input and output requirements, are unique to FpVTE. This custom configuration is implemented via our FpVTE Application version 66 which we offer to make available to authorized Government organizations which wish to replicate our FpVTE configuration.

bioscrypt

FpVTE System Description Document

October 2003

Overview

Bioscrypt's verification library, Bioscrypt Core, is a sophisticated, state-of-the-art algorithm for comparing fingerprint images. It can be found at the heart of all Bioscrypt product offerings and is also available for license.

Bioscrypt Core is proven technology. It is the engine behind the over 55,000 Bioscrypt physical access products that have been deployed to organizations such as NASA, New York City Police Department, American Express, E*Trade, and Continental Airlines. Over 100,000 Network Access stations, including Targus fingerprint capture devices rely on Bioscrypt Core. Additionally, it has been selected by various fingerprint sensor manufacturers such as Atmel, Authentec and Fidelica, and application developers such as Indivos and Sense Technologies.

Features

Flexibility

Bioscrypt Core can be customized for particular applications, taking into account platform requirements, security concerns, template size restrictions, search speed, and database size requirements.

Platform Interoperability

Bioscrypt Core has been specifically designed to be portable and has been successfully deployed on numerous operating systems and processing architectures. The library is available for Windows, Windows CE, and Linux, as well as for many popular Digital Signal Processors. The Bioscrypt team has extensive experience with both PC and embedded software development. Over the past seven years, Bioscrypt has developed products using Texas Instruments, Analog Devices, and Motorola DSPs.

Sensor Interoperability

Bioscrypt pioneered sensor interoperability to ensure flexibility across sensor offerings. Today, Bioscrypt can support interoperability between all leading sensor types, including offerings from: Atmel, AuthenTec, Cross Match, Delsy, DigitalPersona, Ethentica, Fidelica, Fujitsu, Infineon, Secugen, ST, and Veridicom. Sensor Interoperability means that templates created using any of the above sensors can be verified using any other sensor on the list, allowing the most flexibility now and in the future.

Industry Standard Interfaces

Bioscrypt Core can be provided with support for the BioAPI (ANSI/INCITS 358-2002) or CBEFF (Common Biometric Exchange File Format - NISTIR 6529-2001) industry standards. This allows straightforward integration of Core into an application that currently supports these standards.

User Record Security

Bioscrypt's patented process for protecting user credentials can be included in Core. This functionality is combined with an encryption mechanism to provide a secure and confidential user record that can be freely transported across a network or carried on a card.

Encryption/Digital Signatures

Bioscrypt offers functions such as data encryption or the generation of digital signatures. The inclusion of these functions within Core permits a strong connection between biometric verification and encryption techniques. For example, data can be encrypted or decrypted, or digital signatures can be created, within our solution and controlled by the biometric verification process, providing a secure implementation with powerful non-repudiation capabilities.

Functionality

Bioscrypt Core has three primary functions: Enroll, Verify, and Identify.

Enrollment is the process of registering a user. The Enroll function accepts a raw image as captured from a sensor. The image is processed, enhanced, and then converted to a mathematical model. This model is compressed to create a fingerprint template. The template is returned, along with image statistics reflecting the quality of the enrollment. Subsequent verifications and identifications compare raw images to previously enrolled templates.

Verification is performed in order to validate a user's identity. It consists of comparing a raw candidate image to a previously enrolled template. A score is returned indicating the similarity of the candidate and template. This score can be compared to a threshold to make a yes/no decision.

Identification consists of comparing a raw candidate image to a list of previously enrolled templates. Through a series of screening processes, the algorithm narrows the list of templates to a manageable size. Those templates surviving screening are compared to the candidate and verification scores are provided. A score exceeding a pre-set threshold indicates a positive identification.

Technology

The Bioscrypt Core algorithm was originally developed at Areté Associates, a defense research company with over 25 years of experience in image processing, noise reduction, and pattern recognition associated with advanced sensor systems in use by the U.S. Department of Defense. The fundamental approach applied to developing this technology was to make the most accurate and complete comparison possible.

Methodology

Bioscrypt Core employs a pattern-based approach to fingerprint comparison. This comparison technique is performed in two fundamental blocks: Image Enhancement and Distortion Removal. In each instance that a finger is applied to a fingerprint capture device, the ridge pattern exhibits a different degree of distortion. The key to accurate comparison of the ridge pattern is the ability to ascertain and then remove the relative distortion between the fingerprint template and the candidate fingerprint image.

In contrast to Bioscrypt's pattern-based approach, the vast majority of fingerprint matching techniques currently employed use a minutiae-based approach. With this approach, the fingerprint is reduced to a short list of detail points (ridge endings, bifurcations, bridges, etc). Generally, all other information from the fingerprint is eliminated. For verification, the minutiae list from the candidate is compared to the list from the template and a decision is made based on the amount of overlap.

Image Enhancement

Prior to enrollment or comparison, each fingerprint image is passed through a sophisticated image enhancement routine. During this process, the image is filtered, smoothed, and conditioned to produce a high quality representation of the ridge pattern. Features such as creases, cuts, abrasions, and pores that appear inconsistently or move from place to place within the image are removed.

Distortion Removal

Bioscrypt Core, using a unique and patented approach, aligns every ridge of the candidate image with every ridge of the template image, providing maximum use of the entire fingerprint image. Subsequent to the removal of the distortion, the ridge patterns are correlated, emphasizing areas in which the images are clean and highly complex and down-weighting area where the images are noisy or bland. This technique is termed likelihood detection and is frequently utilized in mission critical U.S. Defense applications.

Patents

Bioscrypt owns exclusive rights to the following two patent families that relate directly to our Core authentication algorithm:

- US Patent 5,909,501, issued June 1 1999: Systems and Methods with Identify Verification by Comparison and interpretation of skin patterns such as fingerprints
- U.S. Patent 6,356,649, issued March 2002: Systems and Methods with Identify Verification by Streamlined Comparison and interpretation of fingerprints and the like

Bioscrypt also owns the following patents relating to the protection of user credentials using a biometric:

- U.S. Patent 5,680,460, issued October 1997: Biometric Controlled Key Generation
- U.S. Patent 6,219,794, issued April 2001: Method for Secure Key Management using a Biometric
- U.S. Patent 6,353,889, issued March 2002: Portable Device and Method for Accessing Data Key Actuated Devices

FpVTE Component List

- Bioscrypt Core for Windows
- Dell Precision Workstation 450
    - Dual Xeon 3.06 GHz
    - 1 GB DDR RAM
    - Windows XP Professional
- Various support applications and scripts that are required to fully automate the testing

Cost Breakdown

Bioscrypt Core is available through the execution of a mutually agreeable license agreement. Upon execution of a licensing agreement, Bioscrypt will commit in writing to a delivery schedule for an optimized version of Bioscrypt Core, including support for and interoperability between sensors/devices/platforms as specified in the license agreement. The licensing agreement usually sets a technology transfer fee, annual maintenance fee, and a per user/transaction royalty. The precise amount of these fees depends on the configuration desired.

The workstation used for this test was purchased for approximately $2900.

Modifications for FpVTE

Bioscrypt Core is provided as a software library. This library was not modified for FpVTE. However, for this test, we wrote a simple application to call the library and we developed several support scripts that were necessary to fully automate the testing.

For further Information

Contact:

Chris Crump, Director of Sales Engineering
Bioscrypt, Inc.
5805 Sepulveda Blvd.
Suite 750
Van Nuys, CA 91411
818-304-7150
www.bioscrypt.com

FpVTE 2003 System Description Document

You have Cogent's written permission to publish the system descriptions in the FpVTE report.
Sonia Anca (12 December, 2003)

Table of Contents

1 Overview of the Systems

Cogent's participation in the Fingerprint Vendor Technology Evaluation 2003 involved the use of the three different systems, SST, MST and LST. The differences between the various systems involved unique algorithms for both feature extraction and match as well as on how to describe and define the features set for finger print images. The software that Cogent Systems used consisted of a command line running under Windows 2000 that was written specially for the Vendor Test using Cogent's Software Development Kits Galaxy V3.2T, V3.2 and V8.60.

1.1 Galaxy V3.2T for SST

This system has been designed for targeting one-to-one verification applications. Since it is assumed that each verification transaction has only one match, we have developed a system that has more complicated algorithms for a higher rate of accuracy. Although this system is more time-consuming, it is aimed at offering more advanced precision in verifying matches.

This system is based on the concept of image matching. As compared to minutia based matching, image matching uses a set of points that are extracted from a print image. The intent of image matching is to use the whole image when matching 2 prints so that a greater amount of information from the fingerprints can be utilized. In this way the image matching process provides much more accurate than can usually be expected. For an enrolled print, the extraction component processes the print image and extracts a small amount of data (called a template) that characterizes the print image. This template would then be stored in the database for future use. When doing verification, the template is then matched against the whole fingerprint image and the matching algorithm tries to find the most accurate match between the input image and the image that is represented by the template data.

The template created by the system would then contain information of the underling image. Template size may vary depending on the application requirements. For a system used in testing, processing a verified print image during matching is prohibited. All images must be processed separately with the template containing more detailed information so that it can serve as an "image" when used to verify a print during matching.

1.2 Galaxy V3.2 for MST

This system has been designed for targeting small to medium scaled AFIS applications or verification applications that need open search capability. Keeping the multi-purpose design in mind, this system has been designed with great flexibility regarding resource requirements (e.g. processor power, memory, etc.) and system speed (including extraction of template, matching templates). Therefore it can be easily configured to fit a wide range of requirements. For applications without many resources, such as those with low-end processors and/or limited memory, the system can be properly trimmed (with minimal cost to performance) to be applicable to the system of this kind.

This system is based on the concept of template matching. For an enrolled print, the extraction component processes the print image and extracts a small amount of data (called a template) that characterizes the print. Only this template will be stored in the database. During verification, the input print is processed in this same way complete with its template extracted. The matching of a print to an enrolled print is done only with their respective templates; no image for either print is involved. This assures a high speed match with the capability of an open search if needed.

The template created by the system is an enhancement of the traditional minutia feature in order to achieve the best performance possible. Template size may vary depending on system configuration and the application requirements, as mentioned above. It may be as small as 500 bytes.

1.3 Galaxy V8.60 LST

This system has been designed for targeting medium to large scaled AFIS applications combined with our hardware search engine. Keeping the multi-purpose design in mind, this system has been constructed with greater flexibility on resource requirement (e.g. processor power, memory, etc.) and system speed (including extraction of template, matching templates). Therefore it can be configured easily to fit a wide range of requirements.

This system is based on the concept of minutiae matching. For an enrolled print, the extraction component processes the print image and extracts a small amount of data that characterizes the print. Only this minutia will be stored in the database. During verification, the input print is processed in this same way complete with its minutiae extracted. The matching of a print to an enrolled print is done only with their respective templates. This assures a high speed match with the capability of an open search if needed.

2 Component list and cost breakdown

The system submitted consisted of both Cogent software and common hardware.

2.1 System for SST

Component	Quantity	Price
IBM xSeries 335 Server Dual CPU 3.0GHz 1024 Mb Memory	1	$4500
Cogent feature extraction software	1	N/A
Cogent one to one match software	1	N/A
Cogent WSQ decompress software	1	N/A

2.2 System for MST

Component	Quantity	Price
IBM xSeries 335 Server Dual CPU 3.0GHz 1024 Mb Memory	1	$4500
Cogent feature extraction software	1	N/A
Cogent one to one match software	1	N/A
Cogent WSQ decompress software	1	N/A

2.3 System for LST

Component	Quantity	Price
IBM xSeries 335 Server Dual CPU 3.0GHz 1024 Mb Memory	6	$27000
Cisco Catalyst 2970 Gigabit Switches	1	$2800
Cogent feature extraction software	6	N/A
Cogent one to many match software	6	N/A
Cogent WSQ decompress software	6	N/A

3 Modifications for the Purpose of FpVTE 2003

Test applications were written to perform small, medium and large tests. The following functions are specifically for the FpVTE 2003 test:

- Reading and parsing the FpVTE 2003 target and query XML files.
- Crash recovery from power outages or other system problems during the test.
- Output similarity matrix in the binary files conforming to the FpVET 2003 test specifications.
- Software used for larger tests.

System Description Document
FpVTE 2003

1. Overview

With over 20 years of international experience, Dermalog is a German based company and a world leader for biometric identification and provider of large-scale AFIS solutions. As a pioneer in biometric identification, Dermalog is one of the providers with the broadest product range in this field available today, with many installations across the globe.

Coding: In about 80 different steps, the fingerprint image is enhanced, binarized, and transformed to a fingerprint template. The resulting fingerprint template is a data structure, including coordinates and angles of the fingerprint's minutiae, coordinates and angles of the fingerprint's cores and deltas, as well as additional pre-filtering information, such as the fingerprint type according to the ANSI/NIST standard. The size of the fingerprint template can be scaled to different requirements; this is a performance vs. size trade-off. For AFIS applications, uncompressed fingerprint templates are used. Their average size is in the range from 1 to 2 kilobytes.

Fingerprint quality: The fingerprint quality resulting from the coding process indicates the usability of the coded fingerprint. The quality is in the range from 0 to 100, the higher the better. Very low-quality fingerprints (quality less than 20) will be rejected and normally have to be enrolled again.

Minutia matching between two fingerprints combines three features: global similarity checks, local similarity checks and heuristics to increase matching speed. The matching is symmetric. That means the scores received by matching Finger 1 with Finger 2 are identical with the scores received by matching Finger 2 with Finger 1.

Dermalog Afis is designed for hardware- and operating system independency. For this evaluation, we work with standard PC hardware and a Windows operating system. Though Dermalog Fingerprint technology is mainly used in large Afis-installations, it can be scaled from small systems on a single PC up to large installations with millions of persons stored. The main features include:

- Very large range of supported capturing devices (high flexibility concerning image size, DPI, and image characteristics like brightness or contrast).
- The kernel is independent of used operating system (Windows NT / 2000 / XP, Solaris, Linux, IBM AIX, etc.) as well as the computer-hardware: Every computer, which is supported by a C++ compiler, could be utilized.
- Dermalog Afis is 100% software based. No proprietary hardware is used (for example no proprietary processor cards, matching accelerators, etc.). This makes it possible to use existing hardware or choose the one with best local support, price, or administration experience.
- High interoperability with existing systems: All Dermalog fingerprint modules can accept fingerprint templates in either Dermalog proprietary or standard ANSI/NIST format. Fingerprint templates produced by the Dermalog encoding-module can also be exported to the standard ANSI/NIST format.
- Fully automated processing without necessity of any manual quality control, but on the same time possibility to work together with manually generated input. For example a latent fingerprint found on a structured background like a banknote can be edited manually, and afterwards compared to the database as if the algorithm had characterized it.
- State of the art fingerprint characterization technology.
- Very fast, reliable, and flexible finger template matcher, that works together with templates from different sources (automatically coded, manually edited, or imported from other minutia based fingerprint identification systems).
- Full 360° rotational invariance: Rotating and shifting of the finger in any direction does not influence the matching result.
- Powerful prefiltering technology: Based on core, delta and pattern type information, a large part of the query set can be eliminated in this early processing step. Thus matching speed can be increased drastically.

2. Component list for the system to be evaluated

- Hardware: 6 standard single CPU PCs (Shuttle Barebones) connected with 100Mbit Ethernet-switch.
- Operating System: Windows XP professional (Service Pack 1a).
- Afis software: DermalogFingerCode3 kernel
- Benchmark-Application (for XML-script-parsing, and workload balancing)
- Aware WSQ. For this test, we chose the Aware implementation of WSQ, since it is certified. Alternative WSQ implementations would be usable, too.

3. Cost breakdown of the submitted system

Dermalog's part:

- Afis server license

Here: for 65,000 person records: **70,000 €**

- Afis client license (distributed coding and/or matching)

5 clients à 5,000 € = **25,000 €**

- Afis workstation license

No workstations required for this benchmark.

- Customisation

Costs for customisation have not been recorded for this benchmark. They are indicated individually, after the customer states requirements.

- System integration support and training

Neither integration into an existing system nor training had to be performed.

- Support

No costs for support in this benchmark.

Hardware costs:

- Computers, switch, uninterruptible power supply, cables

For this benchmark approx. **7,000 €**

- Additional hardware (Live scanners, flatbed scanners, etc.)

No additional hardware used in this benchmark.

3rd Party licenses:

- License for the operating-system(s)

MS Windows XP Professional. Others are possible.

- License for WSQ

Aware WSQ. Others are possible.

- License for database-software

Various options. No database software included for this benchmark.

Sum of costs: 102,000 € plus (if desired) costs for 3rd party licenses, additional hardware, and additional work to be performed.

4. Modifications required to take FpVTE 2003

There were no modifications necessary to the Afis-engine. The Afis front-end has been replaced with the required XML-script interpreting benchmarking tool:

- The functionality for evaluation of simple XML scripts had been built from scratch.
- In contrast to a usual Afis application, this benchmarking tool does not utilize any database.
- The benchmarking tool uses its own workload balancing algorithms (distributed computing).
- The required components (md5 support, wsq, Ansi/Nist, coding (=characterization), prefiltering, matching) had been integrated.

SYSTEMS DESCRIPTION DOCUMENT
FpVTE

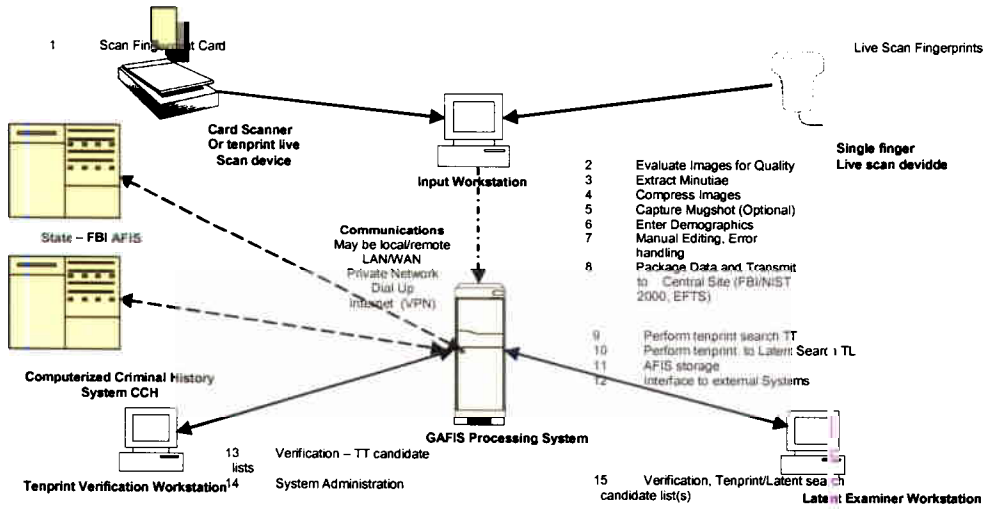
INTRODUCTION

Golden Finger's GAFIS is a fingerprint processing system built on advanced algorithms for fingerprint feature detection (minutiae and other characteristics) and fingerprint matching. The algorithms can, as they have been for the FpVTE, be implemented on standard Commercial Off The Shelf (COTS) components. For very large configurations with extreme matching requirements, the system can be deployed on cost effective large scale specialized hardware.

The system was initially designed and implemented for use in the technically demanding police environment. Here, matching accuracy must be combined with an ability to develop and maintain very large files, perform well with less than perfect image data, and operate well in a networked environment. The system meets these challenges.

Following are two flow diagrams outlining the principal processing in a criminal justice environment – for Tenprint identification processing and for latent criminal search processing:

Criminal AFIS Processing
Tenprint Processing Flow

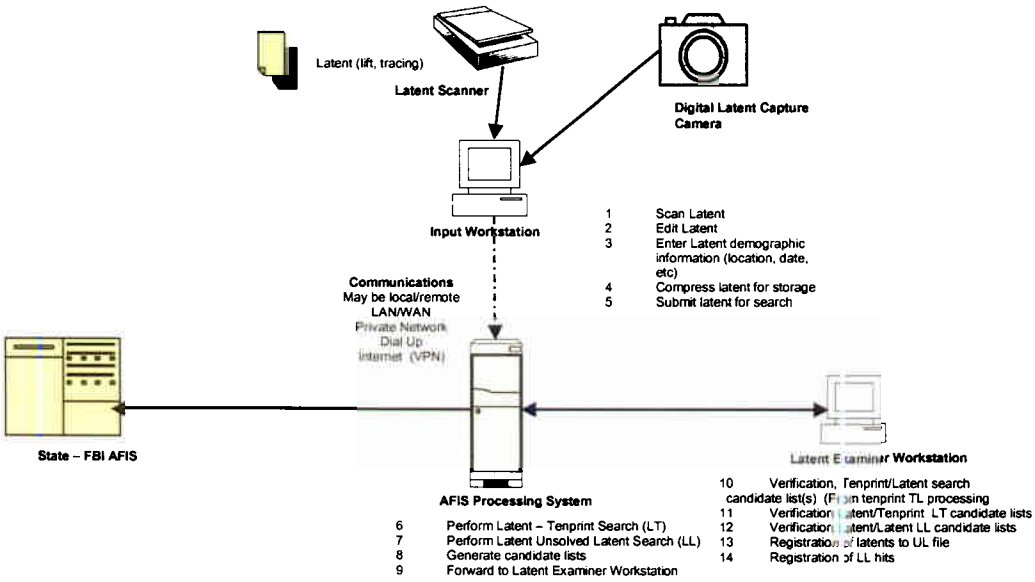


Addr: 55E Huntington Dr, Suite 320,
Arcadia, CA, 91006
http://www.goldenfingersys.com

Tel: 1 (626) 446-8826 Fax: 1 (626) 446-8977

Email: Michael@goldenfinger.net

Criminal AFIS Processing
Latent Processing Flow



The tenprint and latent operations work as an integrated system, combining the build, maintenance, and search of both identification (tenprint) and crime scene (latent) processing.

The building blocks which serve as the foundation for the GAFIS criminal justice applications can be used in the development of a wide variety of applications. These range from simple identify verification processes used in access control to large scale civil applications for both commercial and government applications such as border monitoring. Largely hardware independent, the building blocks include:

- Finger image capture (live scan or scanned ink)
- Finger image processing – finger print analysis and minutiae detection
- Fingerprint matching
  - Simple one:one matching
  - Simple database search – one:many
  - Complex search – fingerprint sets against sets (e.g. tenprint searches)
- Presentation of search/match results for reporting and human verification.

Addr: 55E Huntington Dr, Suite 320,
Arcadia, CA, 91006
http://www.goldenfingersys.com

Tel: 1 (626) 446-8826 Fax: 1 (626) 446-8977

Email: Michael@goldenfinger.net

SYSTEM OVERVIEW – FpTVE

The same GAFIS hardware configuration and operating software are employed for both the MST and LST components of the FpTVE test. The hardware consists of four standard commercially available dual processor SMP computers utilizing Intel Xeon 2.8 GHz processors. The operating environment is MPI (Message Passing Interface) standard and Microsoft .NET framework. A summary configuration follows; costs are current commercially quoted retail prices.

Component List – FpTVE
Hardware

Quantity	Item	Details	Unit Price	Total Price
4	Dell PowerEdge 1750 rack mount server	Two Intel Xeon 2.80GHz Processors, 533MHz FSB, 512kB Cache, Hyper-threading Enabled 1.0 GB Memory 36.0 GB Ultra320 10,000rpm Hard Drive Intel Pro 1000XT Gigabit NIC-Copper	$2,200	$8,800
1	3Com® Baseline 10/100/1000 Switch 8-Port	Gigabit unmanaged workgroup switch, rack-mount	$500	$500
1	APC 2200VA UPS	RackmountG3, 120V, 2200VA, 2U Rack mount	$950	$950
1	DELL PowerEdge Rack 2410	24U Short rack	$850	$850
1	DELL KVM Switch	8 port keyboard / video / mouse switch	$700	$700
1	DELL 16A PDU	120V, 16Amp power distribute unit	$80	$80
1	External CD-RW	52X/24X/52X CDRW USB 2.0 with software	$ 60	$160
1	Monitor	DELL 15" Flat Panel	$280	$280
1	Keyboard and Mouse		$300	$300
TOTAL				$12,620

Software

Quantity	Item	Description		
4	Microsoft Windows 2003 Enterprise Server	Operating System	$3,599	$14,396
4	Microsoft .NET Frameworks 1.1		Public Domain	N/A
4	NT-MPICH 1.3.0-a	MPI Implementation for NT based SMP clusters	Public Domain	N/A

Addr: 55E Huntington Dr, Suite 320, Arcadia, CA, 91006
http://www.goldenfingersys.com
Tel: 1 (626) 446-8826 Fax: 1 (626) 446-8977
Email: Michael@goldenfinger.net

1	Golden Finger System GAFIS 5.0 Engine Network Edition	Fingerprint engine, Includes all fingerprint functions including image processing, fingerprint matching, and database management. System pricing is based on database size and matching speed required. Please see comments below.	$40,000	$40,000
1	Perl 5.8.0 for Windows	Perl required by validate.pl	Public Domain	N/A
1	Symantec AntiVirus Corporate Edition 8.0 with 5 clients	Virus checker	$270	$270
TOTAL				$54,666

Note on cost/Pricing

Pricing for the Golden Finger GAFIS Network Engine is based on the following factors:

- Database Size
- Matching requirements (number and type of matchers employed)
- Functions performed – capabilities used

The $40,000 pricing for the GAFIS software configuration above is based on a database population of 65,000 individuals who will have from one to 10 finger images per member. The matching configuration, hardware and software, is based on an estimated 2.3 Billion matches (ranging from single matches to tenprint matches) over a 21 day period and operating with four dual processors for matching throughput. Functions include finger image processing, matching, and limited database management.

Example criminal justice systems will have estimated basic software prices of approximately:

Database	Price
50,000	$25,000
250,000	$75,000
500,000	$150,000

Included in the pricing would be the full functions described in the Criminal AFIS Tenprint and Latent processing flowcharts above. Final pricing would be based on the actual configuration and the amount of customization and support required.

MODIFICATIONS REQUIRED TO TAKE THE FpTVE

The specific hardware configuration and application software were developed to meet the test system design and the performance requirements needed to comply with the testing schedule, specifically of the LST.

Addr: 55E Huntington Dr, Suite 320, Arcadia, CA, 91006
http://www.goldenfingersys.com
Tel: 1 (626) 446-8826 Fax: 1 (626) 446-8977
Email: Michael@goldenfinger.net

All hardware and operating software is COTS with no special configurations or modifications. The application software to run both the MST and LST is based on standard Golden Finger GAFIS components.

Addr: 55E Huntington Dr, Suite 320,
Arcadia, CA, 91006
http://www.goldenfingersys.com

Tel: 1 (626) 446-8826 Fax: 1 (626) 446-8977

Email: Michael@goldenfinger.ne:

FpVTE 2003 System Description

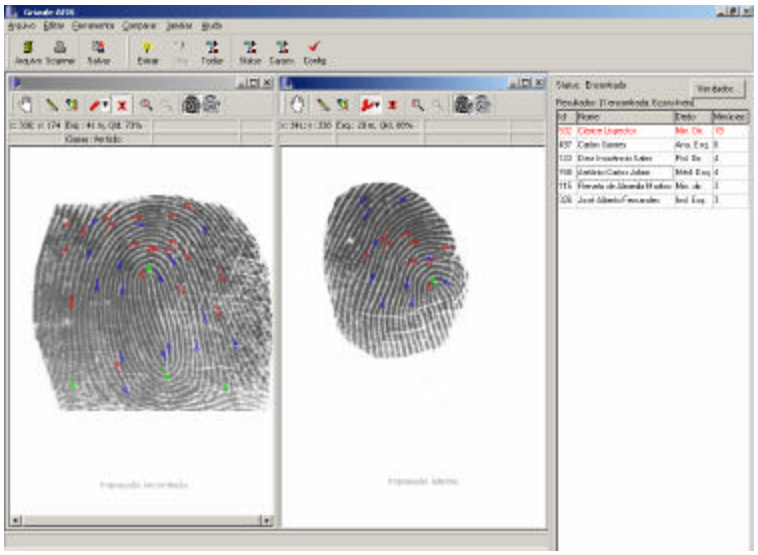
Company

Griaule is a leading AFIS software components supplier in Brazil, with Customers in 6 states, some of them with more than 500.000 people enrolled. We are a company linked to State University of Campinas, UNICAMP, one of the largest universities in Latin America with more than 3.000 researchers covering almost all areas of knowledge

Our core business is the development of new methods and new AFIS search engines for the optimization of AFIS applications and fingerprint image storage.
Griaule possess a unique know-how on cluster computer architecture that reduces searching time using less computer power.

Technology

The purpose of our products is to combat fraud by identifying people on the basis of their unique fingerprint features. Among applications currently in use are unified database of civil and criminal files, prison management, issuing of ID cards and driver's licenses.



Our products are extremely oriented toward performance, stability, and reliability. Our solutions comfortably handle small to gigantic databases containing hundreds of millions of fingerprints.

Products

Griaule AFIS: is a full suite of components for public safety and identification in the Internet and WEB environments compliant with FBI's WSQ and ANSI/NIST standards, primary classification, ten-print search, one-print search and latent search.

Griaule Capture Objects: Components for digital capturing of images from paper or live, such as photographs, fingerprints, signatures, digitizing of documents, latent prints, and ten-print cards.

Griaule Printing Objects: Components for printing ID cards, ten-print cards, and civil and criminal records.

Griaule SpeedCluster: High availability and scalability cluster manager for extremely quick searches of fingerprints allowing searches in databases containing millions of entries to be completed within seconds. The SpeedCluster is tolerant to computer faults, and automatically redistributes the workload to remaining computers without user intervention.

Itautec InfoCluster: High availability and scalability cluster. Composed by 10 dual XEON Itautec Infoservers, Gigabit Switch, KVM, Monitor and 3 KVA UPS.

Integrators

Griaule provides its systems through integrators, which are companies capable of providing full solutions including network infrastructure, telecommunications, servers, workstations, training, specific development, personnel allocation, technical assistance and support.

Overview of submitted systems

Griaule submitted for FpVTE 2003 the "Griaule AFIS" and "SpeedCluster" software, and Itautec Infocluster hardware, participating in the Large Scale Test (LST) only.

The WSQ algorithm is a component of Griaule AFIS and is certified by FBI, certification number is #1279.

It was also developed a specific application, the FpVTE Manager to meet the FpVTE 2003 specifications.

Component list and cost breakdown

Itautec InfoCluster

Quantity	Specification	Unity Price (US$)**	Total Price (US$)**
10	**Itautec* Infoserver** Dual Xeon 2.6 GHz processor 02 GB RAM 01 HD SCSI 72 GB	3,000.00	30,000.00
01	15" Monitor	200.00	200.00
01	KVM Switch	600.00	600.00
01	Ethernet Gigabit Switch	1000.00	1000.00
01	3KVA UPS	1000.00	1000.00
01	Software license for Griaule AFIS limited to 298,000 fingerprints enrolled (the target set for LST is 298,000 fingerprints)	29,800.00	29,800.00
		Total (US$)	62,600.00

* Itautec is the largest IT Brazilian Company
** All prices are average prices without tax

Contact

Raquel Lisboa
Sales
+55 (19) 3788-4998
raquel@griaule.com

Identix Corporate Research Center
One Exchange Place, Suite 800
Jersey City, New Jersey 07302
Phone: 201-332-9213
Fax: 201-332-9313
http://www.identix.com
E-mail: info@identix.com

1.0 Overview of Submitted Systems

The technology used in the Fingerprint Vendor Technology Evaluation (FpVTE) 2003 is derived from the algorithms in the BioEngine® Software Developer's Kit (SDK), which contains the very latest in Identix' fingerprint recognition technology.

The BioEngine® SDK contains fingerprint matching capabilities that allow developers to create custom one-to-one verification and one-to-many identification applications, such as time and attendance, transaction verification, physical access, information security and ID programs. The BioEngine SDK is BioAPI compliant.

The BioEngine® SDK has a number of capabilities:

Image Acquisition: Allows acquisition and enhancement of fingerprint images from the Identix' DFR® series of optical readers.

Quality Control: Assesses captured images for existence of a fingerprint, core quality, ridge line quality and overall usefulness of the image for template extraction.

Processing: Converts a fingerprint image into a minutia based template that is typically no more that 500 bytes.

Search: Implements high speed template matching (verification) and template searching (identification).

The BioEngine Match Algorithm

Fingerprints are comprised of various types of ridge patterns: left loop, right loop, arch, whorl and tented arch. The discontinuities that interrupt these smooth ridge patterns are called minutia, which form the basis for fingerprint identification.

The BioEngine match algorithm estimates the quality of the ridgelines and then extracts the points in which the ridges split, intersect or end (minutia). These minutia points are converted into a mathematical code called a template. Matching two minutia-based templates does not require that all extracted minutia match. In fact very strong matches can be made when as few a one third of the total minutia match.

Because minutia points do not change over time and due to the fact that not all minutia must be present in order to verify identity, minutia based systems are the preferred method underlying most fingerprint biometric systems. For example, cuts and scars may not affect all minutia points and even partial prints left behind at crime scenes may yield sufficient amount of minutia points to run a comparison against a database. One of the largest criminal databases in the world, the FBI's IAFIS system with over 40 million records, uses minutia based fingerprint templates.

The Identix BioEngine algorithm is the underlying authentication mechanism for a broad range of verification and identification solutions worldwide, including:

- Brazil – Brasilia Camara de Diputados– time and attendance
- Brazil – Corte Suprema de Justicia – Brasil – verification
- Columbia – Policia Nacional – smart ID
- Dominican Republic – voter registration
- El Salvador – San Salvador drivers' licenses
- India – New Delhi drivers' licenses
- Spain – social security payment disbursement
- South Africa – pension payment disbursement
- U.S. Department of Defense – personnel enrollment and verification
- U.S. Immigration & Naturalization Services - Mexican Border Crossing Card
- U.S. Departments of Motor Vehicles in California, Colorado, Georgia and Texas

Over 100 million BioEngine templates have been issued to date.

2.0 Component List and Cost Breakdown of System

The same system was used for the Medium-Scale Test (MST) and the Large-Scale Test (LST). This system consisted of:

Component	Quantity	Cost (U.S. Dollars)
Identix BioEngine® SDK v4.0 step 1	1	10,000
IBM X Series 8 Blade System	1	50,267
Windows 2000 Advanced Server	1	922
APC SMART-UPS 3000	1	1,092
APC power distribution unit	1	150
Netgear Fast Ethernet Switch FS116	1	73
IOmega USB 250 Drive	1	110
Dell Monitor, Keyboard, and Mouse	1	310
Ethernet cables	2	16
Total Cost		62,940

3.0 Modifications Specifically for FpVTE 2003

No modifications were made to the BioEngine® SDK v4.0 step 1 fingerprint algorithms. In order to take FpVTE 2003 a test application was written that was used for both the MST and LST. The fingerprint algorithms used in this test application were from BioEngine® SDK v4.0 step 1.

The test application included the following functionality:

- Reading and parsing the FpVTE 2003 target and query XML files
- Crash recovery to recover from power outages or other problems during the test
- Support for processing the tests over eight machines in parallel
- Writing binary results files conforming to the FpVTE 2003 specifications
- Writing status information on the Microsoft Windows console and to log files

FpVTE System Description Document for Motorola

The system supplied for the FpVTE test is a slightly modified version of a standard Motorola Omnitrak system available for purchase. Some software was written to run the workflow of the test, read the NIST test definitions and write the score files. The hardware is representative of hardware being shipped to Motorola AFIS customers.

Hardware

The system consists of 15 HP DL360G3's and 1 HP DL380G3. The DL360 nodes have dual Xeon 3.06 GHz processors and are equipped with 3 GB of main memory and a 36 GB disk used for operating system files and temporary workspace.

The DL380 node has dual Xeon 3.06GHz processors and is equipped with a 4 GB of main memory and a 36 GB disk used for operating system files. The DL380 also contains a 600 GB RAID 5 array used for working data storage.

The DL380 and DL360 are connected using gigabit Ethernet as the main network. A secondary 100 megabit Ethernet network is used for out of band lights out management and monitoring functions.

The DL380 is connected to a rack mountable keyboard and LCD monitor combination. The DL360 nodes lack a console connection as all functions can be accomplished via the management network.

The entire array of 16 machines, monitor and keyboard, and network switches are powered by a group of four HP uninterruptible power supplies. The load is distributed among the power supplies, and the DL380 is powered by two different UPS's through its dual redundant power supplies. Each UPS is powered by a single 110V AC circuit.

Software

All of the computers in the system run Windows 2000 Server, though the system can be configured to run Linux also. The hardware used for the FpVTE test was originally purchased as a Linux cluster for research purposes, but was temporarily reallocated to the FpVTE test. It does not differ substantially from the hardware Motorola normally ships to customers.

Each of the DL360 nodes runs a set of matching and image processing services. The DL380 node serves as the master controller for the system and runs a simple workflow manager, data exchange service (to read NIST files), and the standard Omnitrak match controller software. Each of the matching and processing nodes runs largely

independently. The system can tolerate node failure and redistribute processing accordingly with graceful degradation.

The workflow manager reads the FpVTE test definition and database definition XML files and submits them to the workflow manager for processing. The workflow manager, in turn, sends the individual cases for image processing and subsequent searching. A standard data exchange service (DES), translates the data files from NIST format into the Omnitrak data format. The workflow manager receives search results from the match controller and subsequently writes them to the results directory in the score file format.

The major modification made to the standard Omnitrak matching subsystem was the addition of the ability to return a set of scores from the entire matching process. Normally, the system only returns a small, configuration defined number of the top scores for each search, but the FpVTE test procedures required returning scores for all prints in each search.

Bill of Materials

The following is a bill of materials containing a line item description of the hardware used in the test.

Item	Qty	Part Number	Mfg Part Number	Description	List Price
1	1	0496528	322939-002	LC 2016-G 3.06/533-512 US 16 NODE GIGABIT	80,419.00
2	1	3796663	300679-B21	1GB REG PC2100 2X512 ALL	550.00
3	5	0484010	286716-B22	146GB 10K U320 UNI HDD ALL	1,039.00
4	15	0484012	286776-B22	36GB 15K U320 UNI HDD ALL	519.00
5	16	0488128	322472-B21	3.06/533 W/VRM DL360G3	1,099.00
6	1	3721204	J4821A	HP ProCurve Switch XL 100/1000-T Module	1,099.00
7	4	0449472	204404-001	COMPAQ UPS R1500 XR 137	866.00
8	4	0462821	218971-B21	EXTENDED RUNTIME MODULE (ERM) R1500 XR	631.00
9	16	3796664	300680-B21	2GB REG PC2100 2X1GB ALL	1,300.00

NEC Solutions America

System Description Document
FPVTE 2003

October 16, 2003

1 TECHNOLOGY OVERVIEW

NEC is pleased to participate in the Medium Scale Test (MST) and the Large Scale Test (LST) of FpVTE2003.

Since the installation of NEC's first Automated Fingerprint Identification System (AFIS) in 1982, NEC has retained AFIS business leadership by providing the most advanced AFIS solutions in the world.

Based on a still revolutionary Relation Matching Algorithm, NEC has reached the highest levels of matching accuracy in AFIS, proven in operational systems, as well as, benchmarks. The NEC AFIS continually maintains the same high level of accuracy, regardless of the size of the database being accessed.

This drive to refine and perfect AFIS technology, combined with a wealth of experience in operations, has produced the most tested and proven AFIS available in the marketplace today.

2 MATCHING ALGORITHM

NEC has dedicated more than a quarter of a century to providing the most efficient and accurate fingerprint matching solutions. NEC is the first company to develop a still revolutionary Matching Algorithm, which uses ridge counts between minutiae, to compare and match fingerprints based on the ridge count data. The ridge count data, unlike minutia position and direction data, does not change even when fingerprint image data is distorted or twisted. This well proven algorithm is very robust on latent matching and/or low-quality prints.

NEC's algorithm also has an exceptional feature for the utilization of Zone data. Zone (or zonal) data expresses whether or not an area (zone) is to be considered a fingerprint ridge area. The clear zone is the fingerprint area even though it might not include any minutiae. On the other hand, the unclear zone is not considered to be part of the fingerprint area. With zone data, NEC's algorithm can match search and file "area" where minutia does not exist. This is a key feature that improves selectivity and accuracy especially for fingerprint data with fewer numbers of minutiae.

NEC has developed several Matching Algorithms: 1) for matching flat and slap prints, 2) for matching live scanned prints, and 3) for matching palm prints. NEC has extensive experience in selecting and combining suitable algorithms to meet the particular need of a customer.

NEC is also heavily involved in the research and development to improve AFIS technology. NEC continues to look toward the future and strives to improve upon its already proven highly accurate fingerprint systems. Described below are two of NEC's research and development projects currently underway to improve matching accuracy.

One of the projects, in conjunction with NEC's traditional minutia matching algorithms, which NEC is working on, is the introduction of Ridge Flow Matching. This additional process will not only add

confidence to the minutia matching mate confirmation but also help in improving selectivity. Ridge Flow Matching will use the ridge flow data (orientation field data) to confirm the mate print with the search print once minutia matching is conducted.
In the second project, NEC will soon introduce a revolutionary matching improvement in Skeleton Matching. By introducing the Skeleton Matching as a support to our traditional matching methodology, there is definite probability of improving selectivity.

3 OTHER CORE TECHNOLOGIES

NEC has other valuable core technologies, such as Pre-selection, Adaptive Finger Selection, and Dynamic Threshold. These core functions are very useful for anyone seeking a cost effective solution for a large scale AFIS.

Pre-selection

NEC's Pre-selection is a function to minimize total matching cost for transactions with two (2) or more fingers per card (subject). Pre-selection compares fingerprint macro-features such as ridge flow data and core/delta data of each fingerprint. The Pre-selection process is much faster than the minutia matching and it can eliminate the majority of file (data base) prints very quickly.

Adaptive Finger Selection

NEC's Adaptive Finger Selection is another function to minimize total matching for transactions with two (2) or more fingers per card (subject). Adaptive Finger Selection determines which fingers to be matched and how many fingers to be matched after examining both search and file data quality. For cards with low quality data either on the search or file card, this function determines more fingers to be used in matching. For cards with high quality data for both search and file cards, this function determines fewer fingers to be used in matching. The Adaptive Finger Selection can optimize matching cost once required accuracy is given.

Dynamic Threshold

NEC's Dynamic Threshold examines score sequence of 1:N matching results, and determines hit/no-hit probability using the statistical analysis. Dynamic Threshold weeds out all but the most likely candidates so that verification operators do not waste time verifying false hits. The proposed system achieves the highest selectivity of any vendor in accurately differentiating between hits and false hits. This ensures that potential hits are included in the minimum number of candidates, so as to reduce the verification workload.

4 MATCHING SERVERS

NEC has a wide range of matching server solutions depending on the size of a system and required accuracy and functionalities.

SMS/FMP Solution

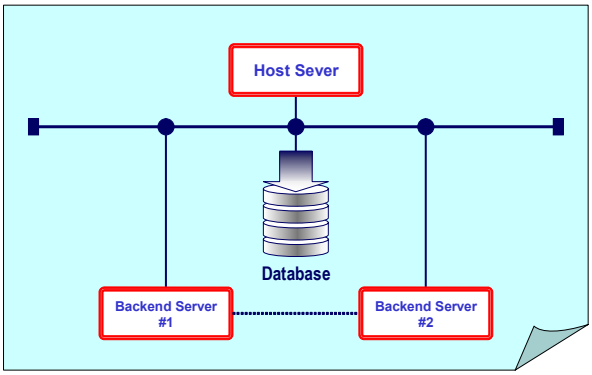
NEC offers the Search/Match Servers (SMS) with Fingerprint Matching Processor (FMP), dedicated hardware, to customers that need cost-effective large-scale systems.

The second advantage of the SMS/FMP solution is its fast response time, i.e. from several seconds to several minutes. Another advantage of the SMS/FMP solution is its very high reliability, which is key for critical 7-day by 24-hour AFIS production sites

Cluster-PC Matching Server Solution

NEC offers Cluster-PC matching servers to customers who need a more flexible matching solution. NEC analyzes the needs of our customers and creates the best solution by selecting the best matching algorithms, and then implementing the selected functionality on the Cluster-PC matching servers.

The Cluster-PC matching server consists of a Host Server and Backend Servers. The Host Server is connected to the Backend Servers through a LAN. The Host Server manages the matching requests and distributes the matching requests to the Backend Servers and then accumulates matching results. The Host Server also manages image-processing requests, and distributes these requests to the Backend Servers. The Host Server also manages a temporary database.



Cluster-PC Matching Server

5 COMPONENTS & COST

NEC selected the Cluster-PC matching servers solution for the FpVTE2003 Test. This solution was selected because of the complicated tests such as matching among 10-finger cards, 8-finger cards, 4-finger cards, 2-finger cards and 1-finger cards.

Since FpVTE2003 intends to evaluate only accuracy not cost-effectiveness, matching cost or speed, NEC has decided to utilize an accuracy-oriented system for the test. NEC will not use Pre-selection or Adaptive Finger Selection on the FpVTE2003 testing. NEC has also decided to use the maximum combination of matching algorithms, including a more time-consuming algorithm to further improve accuracy. Listed below are the costs for FpVTE2003 test system.

Cluster-PC Matching Server for MST

No.	Component	Quantity	Cost
1	Host Server Dell Precision Workstation 450 - CPU: Dual Intel Xeon 3.06GHz - Memory 2GB - 40GB First Disk Drive - 80GB Second Disk Drive	1	$5,500 (*1)
2	Backend Server Dell Precision Workstation 450 - CPU: Dual Intel Xeon 3.06GHz - Memory 1GB - 40GB First Disk Drive - 80GB Second Disk Drive	2	$11,000 (*1)
3	Monitor NEC/Mitsubishi LCD 1850	1	$800 (*1)
4	UPS APC SUA1500	2	$1740 (*1)
5	HUB Dell Powerconnect 5212	1	$2,000 (*1)
6	Cluster-PC Matching Server Software MST	1	N/A (*2)

Note (*1): Hardware pricing includes assembling, software loading, Off Site testing, and shipping and installation

Note (*2): Software Costs are quoted separately based on particular requirements of each customer.

Cluster-PC Matching Server for LST

No.	Component	Quantity	Cost
1	Host Server Dell Precision Workstation 450 - CPU: Dual Intel Xeon 3.06GHz - Memory 2GB - 40GB First Disk Drive - 80GB Second Disk Drive	1	$5,500 (*1)
2	Backend Server Dell Precision Workstation 450 - CPU: Dual Intel Xeon 3.06GHz - Memory 1GB - 40GB First Disk Drive - 80GB Second Disk Drive	9	$49,500 (*1)
3	Monitor NEC/Mitsubishi LCD 1850	1	$800 (*1)
4	UPS APC SUA1500	5	$4350 (*1)
5	HUB Dell PowerConnect 5212	1	$2,000 (*1)
6	Cluster-PC Matching Server Software LST	1	N/A (*2)

Note (*1): Hardware pricing includes assembling, software loading, Off Site testing, and shipping and installation

Note (*2): Software Costs are quoted separately based on particular requirements of each customer.

6 SPECIAL MODIFICATIONS FOR FPVTE2003 TEST

The following specific test application was developed to conduct both MST and LST.

1. Reading and parsing the XML files defined for FpVTE Target and Query data
2. Managing LST 31 subtests over multiple Backend Servers
3. Writing score files defined by FpVTE

NEUROtechnologija Ltd.
Ateities 10, Vilnius 2057, Lithuania, Phone: +370 5 2773315, Fax: +370 5 2773316, http://www.neurotechnologija.com

VeriFinger System Description

1. Overview of the submitted system

In the FpVTE 2003 Neurotechnologija Ltd. has submitted the fingerprint identification engine **VeriFinger**, intended for biometric system developers and integrators. The FpVTE 2003 test system was run on a personal computer working under Windows XP Professional and using VeriFinger 4.2 software.

The VeriFinger fingerprint recognition algorithm follows the commonly accepted fingerprint identification scheme, which uses a set of specific fingerprint points (*minutiae*). However, it contains many original algorithmic solutions, which enhance the system performance and reliability. Some of them are listed below:
Adaptive image filtration algorithm which eliminates noise, ridge ruptures, stuck ridges and extracts minutiae reliably even from poor quality fingerprints, with processing time of about 0.2 - 0.4 seconds.
The VeriFinger matching algorithm contains both 1:1 (verification), and 1:N (identification) modes. The algorithm is fully tolerant to fingerprint translation and rotation. Such tolerance is usually attained by using the Hough Transform-based algorithms, but this method is quite slow and unreliable. VeriFinger uses an original fingerprint matching algorithm instead, which currently enables the achievement of fast matching and identifying of fingerprints even if they are rotated, translated and have only 5 – 7 similar minutiae (usually fingerprints of the same finger have 20 – 40 similar minutiae).
VeriFinger does not require the presence of a fingerprint core or delta points in the image, and can recognize the fingerprint from any part of it. However, if these points are present, it uses them for more reliable recognition.
VeriFinger can use database entries which were pre-sorted using certain global features. Fingerprint matching can then be performed first with the database entries having global features most similar to those of the test fingerprint. If matching within this group yields no positive result, then the next record with most similar global features is selected, and so on, until the matching is successful or the end of the database is reached. In most cases the correct match will be found at the beginning of the search. As a result, the number of comparisons required to achieve fingerprint identification decreases drastically, and correspondingly, the effective matching speed increases.
VeriFinger has a fingerprint enrollment with features' generalization mode. This mode enables the collection of generalized fingerprint features from three fingerprints of the same finger. Each fingerprint image is processed and features are extracted. Then the three collections of features are analyzed and combined into a single generalized features collection which is then written to the database. This way, the enrolled minutiae are more reliable and the fingerprint recognition quality considerably increases using this enrollment mode.

VeriFinger includes algorithm modes that help to achieve better results for specific scanners.

VeriFinger is available for developers and system integrators as a Software Development Kit or in its Source Code version. The VeriFinger software allows rapid algorithm integration into biometric enabled applications. VeriFinger is available for MS Windows, MS Windows CE 3.0 and Linux.

2. Component list of the system to be evaluated

VeriFinger can work on different hardware and software platforms. In the FpVTE 2003 VeriFinger is presented using the following configuration:

Hardware:

Desktop PC, 2.6 GHZ Pentium 4 Hyperthreading,
512 MB DDR SDRAM (400 GHZ),
Dual 40 GB Western Digital Hard Drives w/ 8 MB cache, RAID 1 configuration,
Standard keyboard and mouse,
SVGA Monitor,
UPS power backup.

Software:

MS Windows XP Professional.
VeriFinger 4.2 software test version.

3. Cost breakdown for the submitted system

VeriFinger 4.2 is available as Software Development Kits and in Source Code packages.
VeriFinger SDK prices start as low as US$ 299.00. For each VeriFinger based product installation, developers or system integrators will need to obtain additional VeriFinger DLL licenses. DLL license prices are dependent on order quantity and other options and range from US$ 10.00 to US$ 75.00 per installation.
VeriFinger source code package pricing is negotiated on a case by case basis depending on the intended use and the estimated size of the user base.

4. Modifications required to take FpVTE 2003

An application was written using the VeriFinger Standard SDK to perform the Middle Scale Test of FpVTE 2003. The following functionality was incorporated into the application:

- Reading of FpVTE 2003 test, metadata and dataset definitions (XML files)
- Reading of ANSI/NIST files
- Dataset enrollment
- Many-to-Many matching (optimized matching of dataset against itself) using One-to-Many matching feature of VeriFinger SDK
- Writing of similarity and image quality files in FpVTE 2003 format
- Resuming in case of crash due to power outages or other problems
- Status information displaying and logging

NIST Verification Test Bed (VTB)

The NIST VTB is described in the document

> Wilson, Watson, Reedy, Hicklin. *Studies of Fingerprint Matching Using the NIST Verification Test Bed (VTB)* ; NISTIR 7020; 7 July 2003. (ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7020.pdf)

The following summary is taken from that document.

The VTB matcher (Bozorth98) is being made available as public domain source code as part of the revised NIST Fingerprint Image Software (NFIS), in mid-2004.

The VTB is a collection of commercial off the shelf (COTS) computer hardware and a suite of public domain application software, unlike most fingerprint matchers, which are expensive to obtain, and require specialized hardware. The VTB was developed to be a reference matcher that can provide a performance baseline for future analyses of fingerprint matchers, as well as comparative analysis of different sets of fingerprint data.

VTB DESCRIPTION

The VTB is a system comprised of a collection of COTS hardware and public domain software. A general description of what constitutes the VTB is presented in this section.

Hardware description

The VTB is currently comprised of 16 dual-processor personal computers. All nodes are equally equipped with the following hardware:

- Dual 1.8Mhz Intel Xeon Processors with 512K Cache
- 400 MHz system bus
- 1 GB PC800 memory 400MHz ECC
- 64bit Gigabit Network card
- 64bit SCSI adapter card
- External IDE RAID with SCSI interface
  - 700GB capacity
  - 8-120GB ATA100, 7200RPM drives
  - Raid level 5 with 1 hot spare

Software description

In addition to the Linux operating system (Red Hat Linux 7.2), a suite of NIST application software was installed on each VTB node.

NIST Fingerprint Image Software

The NIST Fingerprint Image Software (NFIS) provides many of the fingerprint capabilities required by the VTB. NFIS is a large public domain source code distribution organized into four major packages:

1. PCASYS (Pattern Classification Automation SYStem) is a neural network based fingerprint pattern classification system;

2. MINDTCT (MINutiae DeTeCTor) is a fingerprint minutiae detector;

3. AN2K (ANSI/NIST 2000) is a reference implementation of the ANSI/NIST 2000 standard; and

4. IMGTOOLS (IMaGe TOOLS) is a collection of image utilities, including encoders and decoders for Baseline and Lossless JPEG and the FBI's Wavelet Scalar Quantization (WSQ) specification.

NFIS is essential to the VTB as fingerprint image files on the VTB are formatted according to ANSI/NIST 2000 and are compressed using WSQ. Minutiae are extracted from fingerprint images using MINDTCT. PCASYS is not used in the VTB.

Four-Finger Plain Segmenter

A key issue to be addressed when considering next generation border control systems is the impact (if any) on searching legacy repositories of rolled impressions with plain impressions captured with live-scan devices. To begin to explore this issue, NIST required a very specific type of fingerprint repository; one where there not only are matched pairs of rolled fingerprints, but that also included pairs of plain impressions mated to rolled impressions. No operational data of this type was available, so NIST needed to quickly and efficiently develop such a repository.

A strategy was developed based on the fact that a standard tenprint card contains a complete set of ten rolled finger impressions, and the same card contains a corresponding set of plain impressions. If one were to extract both sets of fingerprints from the card, then plain versus rolled studies could be conducted. The greatest challenge with this is that two groups (left and right hand) of four fingers (index, middle, ring, and little) are imprinted in a single box on the card. There is one box for the four fingers from the right hand, and a second box for the four fingers from the left hand.

A segmenter was designed to automatically extract plain impressions from an image of a four-finger plain impression box. Commercial segmenters are available, but there were unique requirements that made it necessary for NIST to develop its own technology. Commercial products have been designed to specifically process live-scan images, and they have difficulty handling artifacts in the image such as handwriting, which is common on scanned images of tenprint cards. Commercial products are designed to primarily maximize yield with little feedback to automatically reject questionable segmentations. The NIST segmenter is carefully designed to find a compromise between maximum yield and accurate automatic results. It was anticipated that as many as one million card images would be processed, so complete automation with no manual interaction or verification was critical.

The NIST segmenter uses a down-sampled binary version of the four-finger plain image. A search is made, which includes rotation, for the best fit of four black ridges (fingers) and three white valleys (space between fingers) and if a sufficient fit can not be found the plains are rejected and not used. After finding all four fingers, the fingertips are isolated by a window, sized just large enough to enclose the fingertip. If any errors occur while

trying to isolate the fingertips, or if the final windows do not meet minimum size requirements, the plains are rejected. Finally, each fingerprint is copied from the original four-finger image, without removing rotation, into a new image with white background. Therefore, any pixels not filled by the copy are set to white.

If plain impressions are rejected for any reason, then the entire card is removed from the resulting repository. Using this approach with the NIST segmenter, about 50% of all cards processed are rejected. The high rejection rate is offset by the fact that the remaining results are highly accurate, and no human interaction was required to build the repository.

Bozorth98 Fingerprint Minutiae Matcher

The VTB detects and reports minutiae in a fingerprint image using MINDTCT distributed in NFIS. Minutiae are points in a finger's friction skin where ridges end (called a *ridge ending*) or split (called a ridge *bifurcation*). These features are represented in their most fundamental form as a coordinate point (designating location) and an angle (designating the orientation of local ridge flow).

Once minutiae are extracted, two different finger image impressions can be compared to each other by matching their corresponding sets of minutiae data fundamentally comprised of an x and y coordinate and a theta angle (x,y,?),. The VTB uses a matcher algorithm referred to as the Bozorth98 matcher, which was chosen as the best available fingerprint matcher for which the algorithm and source code were readily available.

The Bozorth98 matcher is an algorithm developed and implemented by Alan Bozorth of the FBI. The algorithm, developed in 1993-95, was designed to match two sets of (x,y,t)'s in such a way as to be rotationally invariant. This capability enables the algorithm to match two fingerprints without the need to first compensate for the fact that the fingerprints may have been captured at varyingly independent orientations.

To accomplish this, the algorithm transforms each fingerprint's set of (x,y,t)'s into a specialized rotationally invariant graph. To compute a match score between two fingerprints, the algorithm iteratively searches between both fingers' graphs for subsets (or subgraphs) that are *compatible*, i.e. coordinate locations and orientations of the minutiae represented within the subgraphs are similar enough to each other based on defined tolerances. The more nodes contained within a compatible subgraph, the higher the accumulated match score. The more subgraphs that are compatible between the two fingerprints, the higher the accumulate match score. The basic algorithm used in the Bozorth98 matcher is a variation of a Hough transform, which has been used as the basis of many fingerprint matchers from the 1980s through the present.

The algorithm is the primary (currently the only) matcher used on the VTB. All results reported in this report were generated using the Bozorth98 matcher. Note that the performance of the Bozorth98 matcher has never been tested against other fingerprint algorithm matchers, and therefore represents an arbitrary baseline.

On the hardware platform mentioned above, the VTB can perform approximately 20,000 fingerprint comparisons per minute, or 30 million comparisons per day.

The Phoenix Group Inc.

The Phoenix Group, Inc. developed AFIX® Fingerprint and Palmprint Matching Software. Their fingerprint matching technology has been used by some of the largest companies in biometric identification for over 10 years.

Besides contract software development for other biometric companies, the primary product The Phoenix Group offers is AFIX Tracker® — a full functioning automated fingerprint / palmprint identification system (AFIS/APIS) sold directly by the company to law enforcement agencies. The main objective for Tracker® is criminal investigation — the most demanding application for fingerprint matching. The Phoenix Group offers several other products built around their fingerprint matching algorithms: AFIX Comparator,® AFIX Verifier,® and AFIX Tracker LE®.

Software for the FpVTE Fingerprint Vendor Technology Evaluation 2003.

Two main components from AFIX Tracker (the extractor and matcher) were used to build the software engine that plotted the minutiae and found matches in the FpVTE. These two components are identical to those built into the current version of AFIX Tracker.®

AFIX Tracker® Automated Fingerprint and Palmprint Identification.

AFIX Tracker® was the first AFIS (Automated Fingerprint Matching System) to run on a Windows® PC and fit within the budgets of most local agencies. It was designed to be used directly by the people who needed computer fingerprint matching technology the most — the investigators and latent print examiners in the field at the local level.

> **"Today, with AFIX Tracker operating in many agencies across the U.S. and abroad, its reputation has been firmly established."**

Algorithms designed for extraction of fingerprint minutiae and pattern matching were designed exclusively by The Phoenix Group Inc. These extracting and matching algorithms have proven successful in the field with investigators and latent print examiners, pointing to fingerprint and palmprint matches that helped solve numerous criminal investigations not solved by existing systems.

Now after AFIX Tracker® has been operating in agencies across the U.S. and thirteen other countries for over 5 years, the validity of the concept of running a local AFIS has been proven, along with the superiority of AFIX Tracker over several other PC based systems that emerged after-the-fact. With a continued barrage of upgrades, including the addition of palmprint capabilities, it is safe to say that AFIX Tracker® represents the state-of-the-art in fingerprint and palmprint matching.

Software Components used in the FpVTE Test

Components pulled from standard AFIX Tracker AFIS software

- AFIX Tracker v4.4 Extractor
- AFIX Tracker v4.4 Matcher

Hardware Components used in the FpVTE Test

Dell Dimension 8300 computer system

- Pentium® 4 Processor at 3.0GHz with 800MHz front side bus
- Memory: 512MB Dual Channel 400MHz DDR SDRAM
- Keyboard: Dell® Quietkey® Keyboard
- Monitors: 18.1 in 1800FP Dell Ultrasharp™ Digital Flat Panel Display
- Video Card: 64MB DDR NVIDIA GeForce4 MX™ Graphics Card with TV-Out
- Hard Drive: 120G RAID 1 (2 x 120GB SATA HDDs)
- Floppy Drive and Additional Storage Devices:3.5 in Floppy Drive
- Operating System: Microsoft® Windows® XP Professional
- Mouse:Logitech® Optical USB Mouse
- Network Interface: Dell Gigabit Ethernet
- Modem: 56K PCI Data/Fax Modem
- CD or DVD Drive: 48x CD-RW Drive with Roxio's Easy CD Creator®
- Sound Card: Integrated 5.1 Audio with Dolby Digital 5.1 capability
- Speakers: Altec Lansing® ADA215 Speakers
- Software Bundles: Microsoft® Office Small Business
- Security Software: Norton Antivirus® 2003 12-month subscription
- Services and Support Options:3 Year Limited Warranty plus 3 Year On-site Service

Additional Components shipped and installed with a standard AFIX Tracker system 9/03/03

Epson Perfection 3200 Scanner
Maxtor 5000XT 250GB External Backup Drive
Epson Stylus C82 inkjet printer
APC Back-UPS 500VA Battery Backup
Premium Support 2-Year Plan (from date of installation)

- All upgrades and new versions of AFIX Tracker® software
- Unlimited technical support calls
- All software maintenance updates
- Free replacement of lost or damaged installation disks

Pricing

U.S. DOLLARS

AFIX Tracker — fully functioning AFIS/APIS — $30,000
Pricing of the standard AFIX Tracker system includes software, hardware (Dell Computer and all periphreals as specified above), installation, on-site training, and 2 year support and free software upgrade plan.

AFIX Tracker L.E. — $5,500
Entry workstation for Tracker plus AFTS/NIST compliant scan and forward system Computer hardware and peripherals included.

AFIX Verifier — $15,500
Software used with single-finger live scan device for instant on-site identity verification. Includes computer hardware, all necessary peripherals, and single-finger live scan device.

Affordable and Upgradable

- Easy to install and maintain. Runs in Windows 98, 2000, XP, or N an off-the-shelf PC.
- Software updates (included in the support package) add new fea keeping pace with suggestions from users, hardware improveme and new operating systems. Capacity of the system can be incre easily by adding larger hard drives and/or multiple systems.

Minutiae-Based Matching

- Classification, core and deltas are not necessary for searching fo possible matches.
- AFIS/APIS (Automated **Fingerprint** and **Palmprint** Identification) fully integrated into one system.
- Networkable — multiple Tracker stations share database
- Add multiple stations at extremely low cost with AFIX Tracker LE store & forward workstation.

Compatible to Accepted Standards

- Send and receive using EFTS/NIST standards.
- FBI certified WSQ compression.
- Classifies prints in NCIC with translation to Henry.

Entry of Prints / Scanning

- Enter fingerprints, palmprints and latents via flatbed scanner, digital camera and live-scan devices. Call for list of compatible live-scan manufacturers.
- Scan ten-print cards in a single scan.
- Single finger replacement. Replace poor-quality rolled impressions with corresponding plain impressions or store both sets of prints.
- Scaling tool corrects scaling when scanning photographed latents or importing images directly from digital cameras.

Biographical Info / Arrest Record

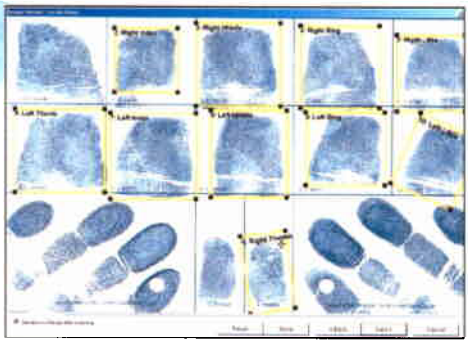
- Allows (but does not require) entry of personal data and criminal history information, including: agency, location, county, state, FBI no., SSN, active warrants, cautions and more. Biographical grid is user customizable.
- Drop-down menu selection of physical attributes.
- Filing of latent fingerprint images by crime scene.

Plotting of Minutiae

- New in version 4.3, AFIX Smart Extract® automatically plots minutiae from rolled prints, plain impressions, palmprints and crime scene latents.
- Allows full user editing of minutiae at every step in the process (plotting, classification, even in the final comparison window). The Latent Print Examiner is always the final judge in plotting minutiae and identifying possible matches.

Working inside AFIX Tracker.

1

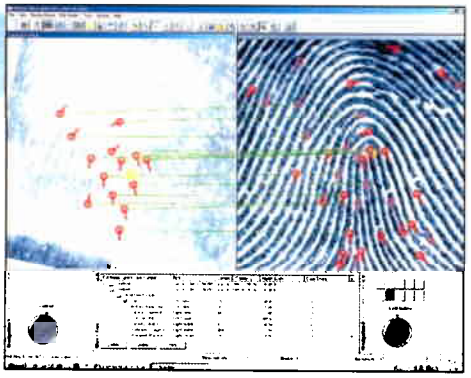


Fast Entry of Ten-prints. *Ten-print cards are entered in a single scan. Finger capture areas can be rotated individually. Templates may be modified and saved. Single finger substitution allows corresponding plain impressions to be substituted for poor quality rolled prints or substitutions from other cards or live scans at a later date. EFTS/NIST files from other AFIS systems or live scan devices can be imported.*

2

AFIX® Smart Extract®. *Minutiae are extracted (or plotted) automatically. The system makes a quality assessment and assigns a value so the user can open cards with lower quality images which may require the examiner's careful eye to edit. Tracker® is unique in allowing the operator to manually edit minutiae at any point in the process, even in the final comparison screen—not possible on many AFIS systems.*

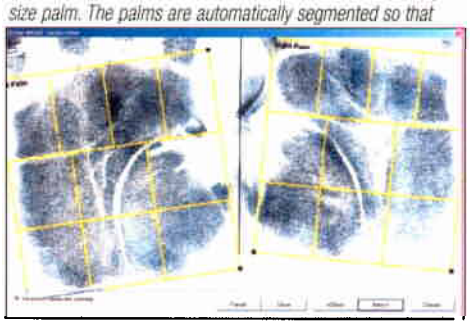
3



The Comparison Window. *Tracker® gives the examiner a candidate list of possible matches. Clicking on a possible match in the hit list displays the two prints in the side-by-side comparison window for verification by the examiner. Comparison lines are drawn between matching points in the two prints. Rotation is automatic. Zoom same and zoom lock make the two prints snap to the same magnification.*

4

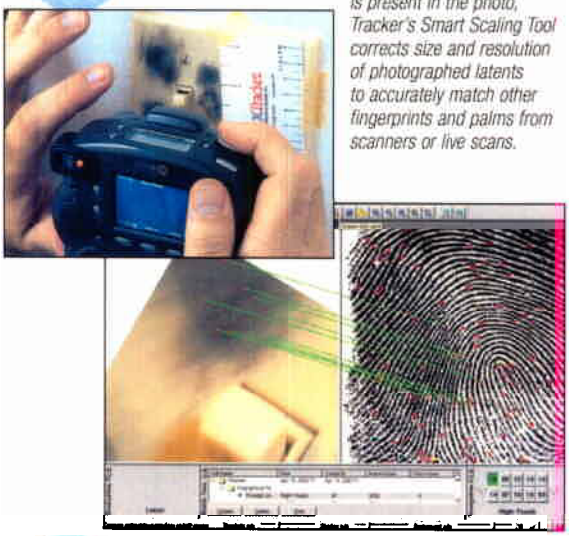
A Palm Interface Designed by Experts with both Experts and New Users in Mind. *Allows for entry of cards with both palms on one side, or one palm on each side. Palm capture box rotates and resizes for accurate capture of any size palm. The palms are automatically segmented so that*



examiners trained and experienced in palm comparison may limit their searches to known areas whenever the latent can be identified. Conversely, all areas may be searched whenever partials are too small to identify or when operators are not as experienced in palm identification. Partials may be searched against fingerprints, palms and even other latents simultaneously.

5

Digital Photographs. *Import latent images directly from a digital camera or scan in conventional photos. If a ruler is present in the photo, Tracker's Smart Scaling Tool corrects size and resolution of photographed latents to accurately match other fingerprints and palms from scanners or live scans.*



6

Tracker® in Action. *Notice in the screen above: A photograph of a latent print on a light switch has been imported directly from the digital camera to AFIX® Tracker®. Within minutes after dusting the fingerprint and photographing it, Tracker's search engine matches it correctly with a print in the database. In the comparison window the latent is automatically rotated into correct orientation. Comparison lines are drawn between matching minutiae in the two prints. The comparison lines can all be turned on automatically, or stepped through one-at-a-time (just as latent print examiners are used to working when searching for unexplainable differences in possible matches). The print comparison can be printed out to be used in interviewing the suspect, added to the case file, submitted to the D.A., etc. The prints can be e-mailed to another examiner for verification. The question is:* ***If you don't have Tracker® in your department, how do you do this?***

Raytheon

Raytheon Company FpVTE 2003 Evaluation System (MST)

Overview

This system is submitted for evaluation purposes only. It represents only the core processing and matching subsystems of our overall criminal AFIS solution.

The general concept used is to distribute the work across several computers and processes using a message -passing interface (MPI). For the MST configuration, two single-processor machines are used. A controlling process resides on one of the machines and directs work to the other processes. This allows for flexible solutions depending on the system needs.

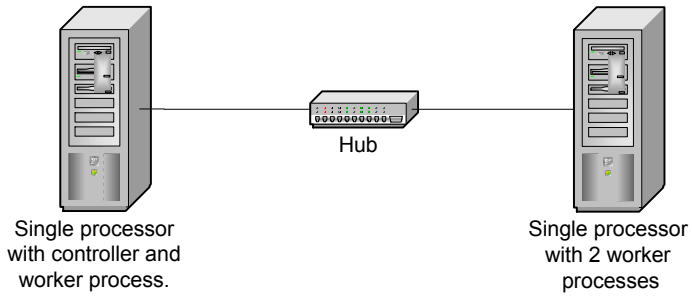


Figure 1 MST Configuration

A two-stage matching process is used for multi-print comparisons.

Components

Software:

- **Microsoft Server 2003 (Standard Edition) –** Operating system
- **Microsoft Visual Studio.Net**. – Used for all custom software applications
- **MPICH** – MPI implementation for parallel processing developed by Argonne National Laboratory.
- **RAYAFIS –** Image processing minutia extraction and matching.

Processing Hardware:

- 2 x HEWLETT-PACKARD D530PC Pentium 4, 2.6 GHz Workstations
  - 80 GB HD
  - 512 MB RAM
- Linksys EtherFast 10/100 5 port hub

Cost Breakdown

Pricing information is not available at current time.

Modifications

Raytheon

Raytheon Criminal AFIS is being developed as a complete collection, analysis, and search solution. The interface to this evaluation system was developed specifically to perform the tasks in FpVTE 2003. The custom applications take the place of the demographic storage and contoller layer which are part of the AFIS Processing Center.

Raytheon Company FpVTE 2003 Evaluation System (LST)

Overview

This system is submitted for evaluation purposes only. It represents only the core processing and matching subsystems of our overall criminal AFIS solution.

The general concept used is to distribute the work across several computers and processes using a message -passing interface (MPI). In the LST configuration, the controlling process is on a machine by itself while the worker processes are distributed among the other machines. This allows for flexible solutions depending on the system needs.

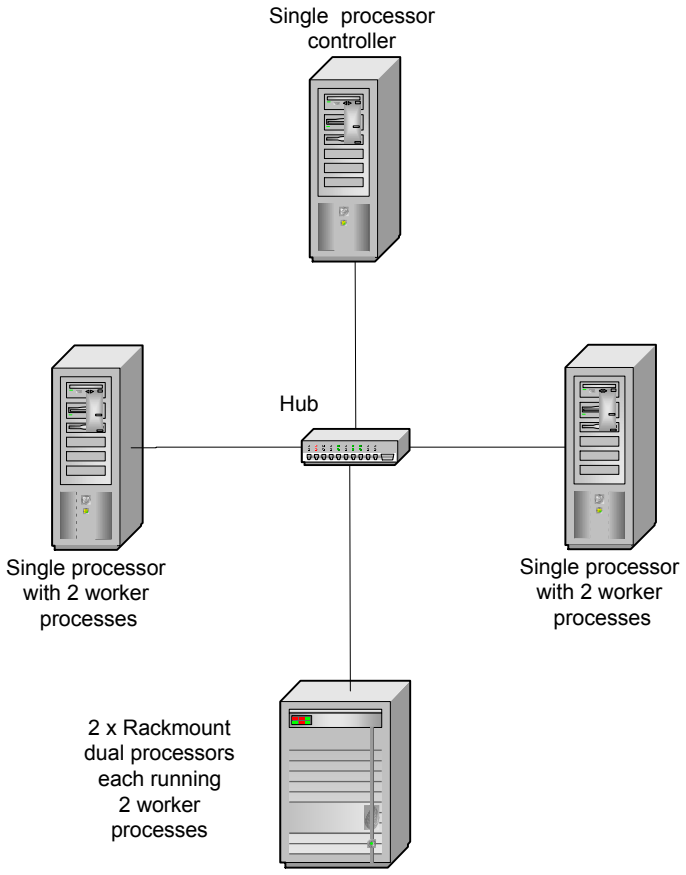


Figure 2 LST Configuration

Raytheon

Components

Software:

- **Microsoft Server 2003 (Standard Edition) –** Operating system
- **Microsoft Visual Studio.Net**. – Used for all custom software applications
- **MPICH** – MPI implementation for parallel processing developed by Argonne National Laboratory.
- **RAYAFIS –** Image processing minutia extraction and matching.

Processing Hardware:

- HEWLETT-PACKARD D51C Pentium 2.4 GHz Workstation
  - 40GB HD
  - 512 MB RAM
- 2 x HEWLETT-PACKARD D530PC Pentium 4 2.6 GHz Workstations
  - 80 GB HD
  - 512 MB RAM
- 2 x HEWLETT-PACKARD DL360R03 X3.06/533 Dual Xeon Rackmounts
  - 70 GB RAID
  - 2 GB RAM
- Linksys EtherFast 10/100 5 port hub

Cost Breakdown

Pricing information is not available at current time.

Modifications

Raytheon Criminal AFIS is being developed as a complete collection, analysis, and search solution. The interface to this evaluation system was developed specifically to perform the tasks in FpVTE 2003. The custom applications take the place of the demographic storage and controller layer that are part of the AFIS Processing Center.

SAGEM MORPHO, INC.

FpVTE 2003
SYSTEM DESCRIPTION DOCUMENT

Version 1.1

SAGEM_MST1

SAGEM_MST2

SAGEM_LST1

SAGEM_LST2

1. Overview of the system to be evaluated

The systems tested in FpVTE are based on the SAGEM MetaMorpho™ commercial AFIS product, linked to a dedicated matching engine set up for the NIST FpVTE tests.

MetaMorpho™ is a complete turnkey biometric identification system that can be configured and customized to meet specific customer requirements. It supports external interfaces to other systems, workstations with user interface functions, image processing subsystems, matching subsystems, workflow management, database management and system administration functions.

Usually an AFIS system is designed to process transactions coming from various sources one after the other, whereas in the FpVTE 2003 evaluation, participants are required to process batches of transactions. Moreover, only a few candidate scores are normally returned to the user, whereas in the FpVTE 2003 evaluation, participants are required to provide as many matching scores as possible.

Hence, the architecture of the AFIS system has been modified in order to take these specific requirements into account. A set of specific control scripts has been developed in order to automate the tests.

SAGEM provided four systems, two for the MST test, and two for the LST test. The four systems are multi-stations, in order to dispatch image processing and matching requests over several “Fingerprint processing” workstations. Hence, every system is composed of a *Workflow Control* station, which supports the MetaMorpho™ AFIS and the control scripts, and of a set of *Fingerprint Processing* stations.

MetaMorpho *Workflow Control station*

- Analyzes test description and starts the appropriate script
- Imports NIST files containing individual records
- Balances feature extractions over several *Fingerprint Processing* stations
- Distributes matching requests to available Fingerprint Processing stations (every station contains the full feature vector database, providing redundancy in case of hardware failure)
- Retrieves result files from Fingerprint Processing stations to build up the similarity matrix
- Creates MD5 files for output

Fingerprint Processing stations

- Decompresses the WSQ fingerprint images
- Extracts the fingerprint features from the image
- Matches the data sets according to the test description file
- Generates the result files

2. Component list for the system to be evaluated

Software
In order to ease system installation, the same software is installed on every machine. It is composed of:

Operating System:
- Microsoft Windows 2000 Professional (Service Pack 2)

Application software:
- MetaMorpho software: MST version 3.1.2A.NST.2A; LST version 3.1.2A.NST.3A)
- Matcher engine (MST version 3.1.2A.NST.2A; LST version 3.1.2A.NST.3A)
- Control scripts (MST version 3.1.2A.NST.2A; LST version 3.1.2A.NST.3A)

COTS software - managed and identified as COTS 3.4.
- Versant 6.0.5
- Apache 1.3.27
- Python 2.2.1
- SWSQ (SAGEM internally developed WSQ library)

COTS communication software
- Ataman 2.4

Hardware
There are two different PC configurations included in each test system:
- Hardware configuration 1 is used for the MetaMorpho workflow station. In one test system, this configuration also holds the fingerprint processing station. There is always one PC for configuration 1 in each test system.
- Hardware configuration 2 is used for the fingerprint processing station(s). There are zero, one or more PC's for configuration 2.

Hardware configuration 1 (workflow control station):
- Pentium IV, 3.0GHz CPU
- 1024MB RAM
- 40 GB Hard Drive
- 2 x 73.6GB SCSI Hard Drives (mirrored)

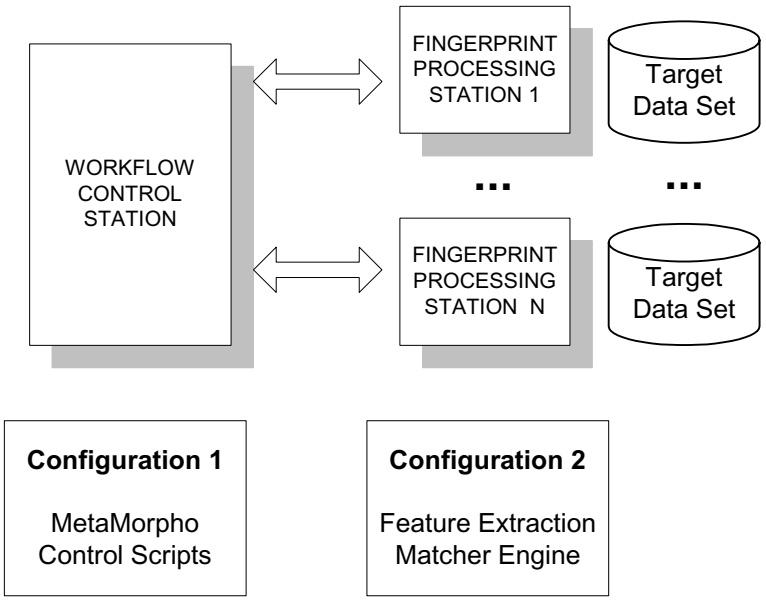
Hardware configuration 2 (fingerprint processing station):
- Pentium IV, 3.0GHz CPU
- 1024MB RAM
- 80 GB Hard Drive

SAGEM_MST1: 1 machine for both *Workflow Control* and *Fingerprint processing*.

SAGEM_MST2: 1 machine for both *Workflow Control* and *Fingerprint processing*.

SAGEM_LST1: 1 *Workflow Control* station and 6 *Fingerprint Processing* stations

SAGEM_LST2: 1 *Workflow Control* station and 2 *Fingerprint Processing* stations



Test System Architecture

3. Detailed cost breakdown of the submitted system

COTS Component Costs

MST1:

Workflow Control PC	*$ 3,500*
Fingerprint Processing PC(s)	*$ 00*
Network Switch	*$ 00*
UPS	*$ 400*
COTS software	*$ 570*
Total:	*$ 4,470*

MST2:

Workflow Control PC	*$ 3,500*
Fingerprint Processing PC(s)	*$ 00*
Network Switch	*$ 00*
UPS	*$ 400*
COTS software	*$ 570*
Total:	*$ 4,470*

LST1:

Workflow Control PC	*$ 3,500*
Fingerprint Processing PC(s)	*$ 6,000*
Network Switch	*$ 200*
UPS	*$ 400*
COTS software	*$ 1,990*
Total:	*$ 12,090*

LST2:

Workflow Control PC	*$ 3,500*
Fingerprint Processing PC(s)	*$ 2,000*
Network Switch	*$ 200*
UPS	*$ 400*
COTS software	*$910*
Total:	*$ 7,010*

Software Licenses

For two reasons, software license cost information cannot be provided in this document.

- SAGEM pricing models are confidential and cannot be provided in a public document.
- The four systems used for these tests integrate specific features that are not yet available in commercial products.

4. Details of any modifications required to take FpVTE 2003.

MetaMorpho *Workflow Control*

- The ANSI/NIST file import function was customized to meet FpVTE specification
- Dedicated scripts were developed for FpVTE tests
- The MetaMorpho workflow was customized

MetaMorpho *Fingerprint Processing*

- The matcher was modified to return as many matching scores as possible
- The matcher parameters were tuned to handle the specific NIST image characteristics (image orientation, quality, …)
- The matcher output was modified to produce the required similarity matrix

Technoimagia

Technoimagia Co., Ltd., 1st BB Building 6F, Ryogoku, Sumida-ku, Tokyo, Japan 130-0026
Telephone: +81(3)5600-0980 Facsimile: +81(3)5600-0981 e-mail: info@technoimagia.co.jp
URL: http://www.technoimagia.co.jp/e_index.htm

1. Overview of Our System for FpVTE2003

We have developed a special version of **FP-Workstation** for *FpVTE2003* to demonstrate the capability of our fingerprint authentication algorithm. The software of **FP-Workstation** is constructed based on our proprietary fingerprint matching tool library, **Fingerprint Authentication System Tool 21("FAST21")**.

What is FAST 21?

- A unique minutiae extraction and matching algorithm for fingerprint identification and verification:
  - *FAST*: Fast processing speed. The proposed **FP-Workstation** recorded approximately 4.5 msec per matching of the preliminary MST sample data set.
  - *ACCURATE*: FAR $\leq$ 0.0001% and FRR $\leq$ 0.05% from 50,000 fingerprints using our optical sensors.
  - *ROBUST*: Immune to the tilted angle of finger (180°) and finger surface conditions (wet/dry).
  - *COMPACT*: Template data size per finger is 128 byte for a standard application. Only 256 bytes for an application that requires 1:N identification with the highest accuracy and the faster processing speed.
  - *EASY TO INTEGRATE*: Can produce the above identification accuracy with any type of fingerprint sensor that can capture a fingerprint image of at least 500 dpi and 256 levels of grayscale.
- Application Program Interface (API) for implementing a versatile fingerprint verification system that is tailored for a particular requirement such as improvement and maintenance of a high security system by adding or embedding API to an existing client system.
- Fast fingerprint 1:N identification algorithm supporting a large-scale central administration system.
  - A high security measure for client-server and web application systems.
- Compact and light software that can be loaded or embedded into various devices.
  - We embedded **FAST21** is in our "**Match on Card**," a smart IC card with ISO7816 compliance.

FAST 21 Library Lineup

The following libraries for Windows and UNIX operating systems can be customized for various devices:

- **FAST-Verify**: Library module for 1:1 fingerprint verification
- **FAST-Identify**: Library module for 1:N fingerprint identification.
- **FP-RADAR BASE**: A plug-in card module for 1:N fingerprint identification engine, and accompanied libraries for controlling the module (for Windows operating systems).

Applications of FAST21

Two working applications are illustrated here:

FP-Security@Station for information security, and **FP-Secure Gate** for physical security.

Case I. FP-Security@Station

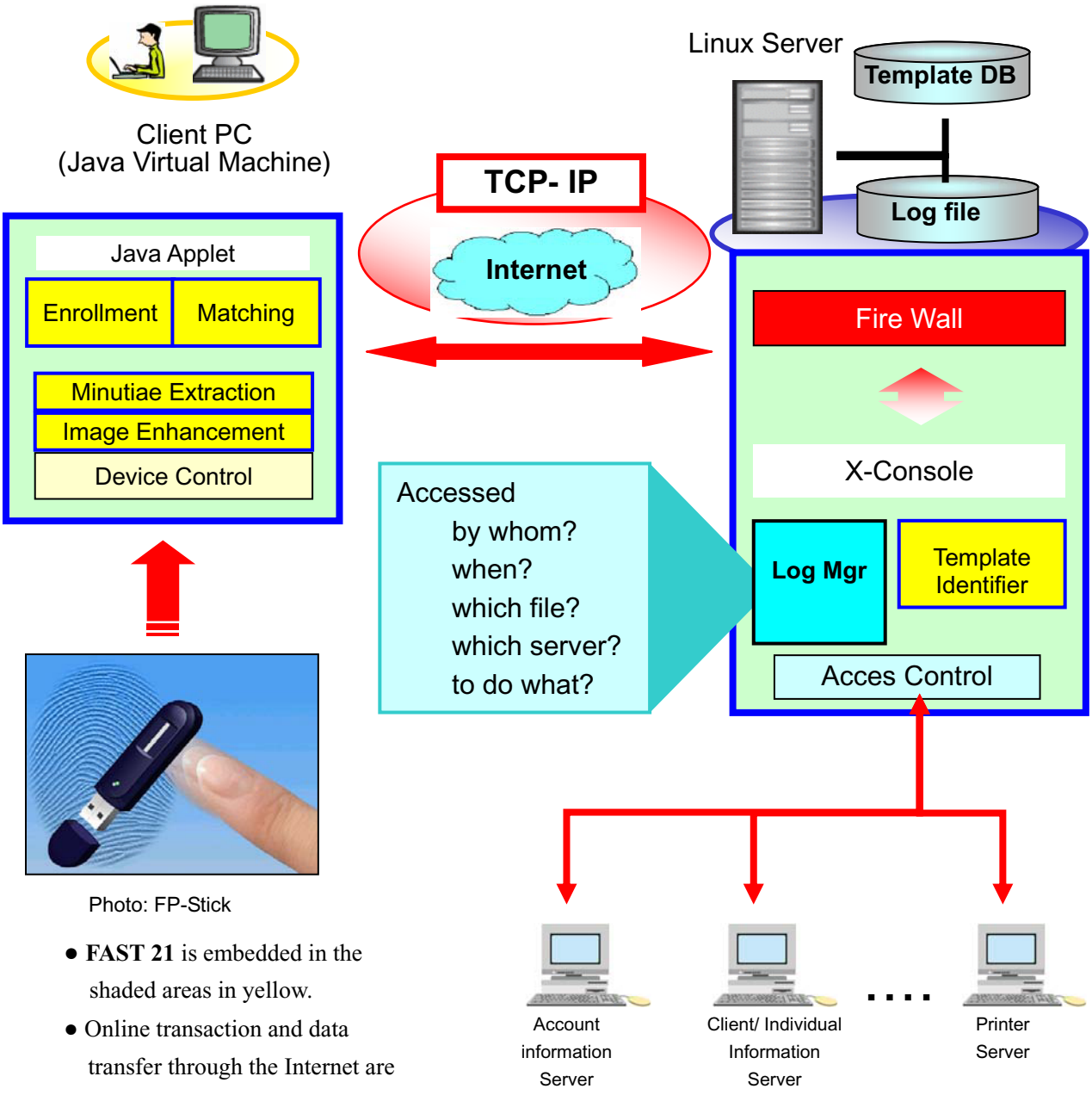


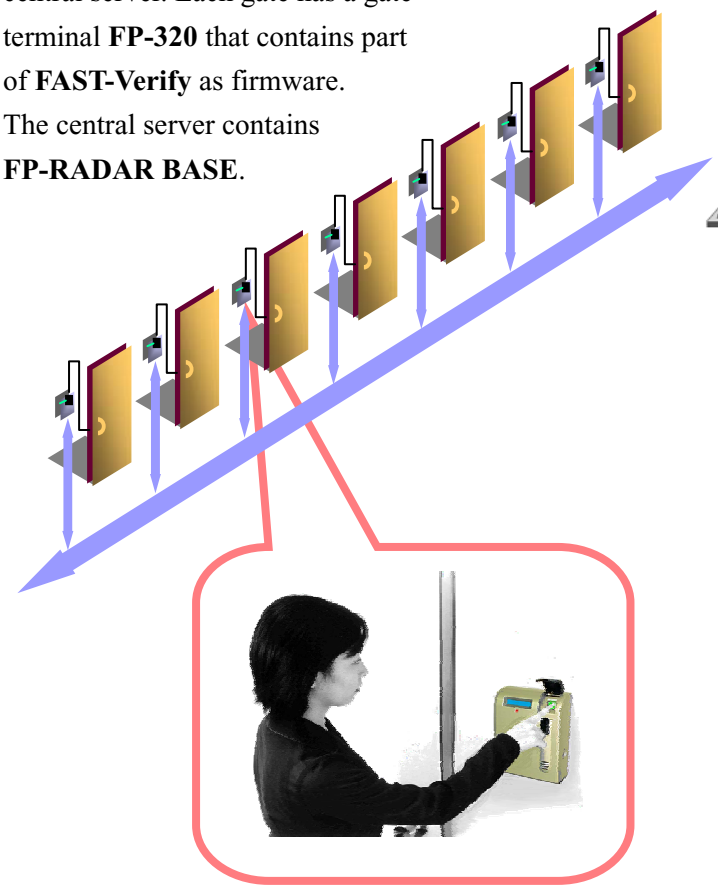
Photo: FP-Stick

- **FAST 21** is embedded in the shaded areas in yellow.
- Online transaction and data transfer through the Internet are secured at user's command.

SECURED INFORMATION EXCHANGE: FP-Security@Station is now officering BCA (Biometrics Certificate Authority) service through the Internet.

Case II. FP-Secure Gate

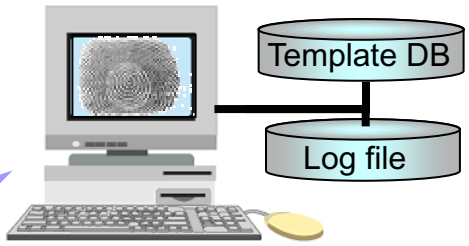
Multiple security gates controlled by a central server. Each gate has a gate terminal **FP-320** that contains part of **FAST-Verify** as firmware. The central server contains **FP-RADAR BASE**.



Each FP-Secure gate terminal has built-in firmware based on **FP-Verify** and an optical sensor. The gate terminal captures and enhances an accesser's fingerprint image to extract characteristics points. Then, the gate terminal creates a template and transmits it to the server, requesting authentication.

KEYLESS ENTRY: with only fingerprint data, the FP-Secure Gate server controls multiple gates to a highly secured areas such as hazardous material storage rooms, controlled medicine rooms, weapon depots, and corporate intellectual property rooms. FP-Gate Server is scalable.

FP-Secure Gate Server

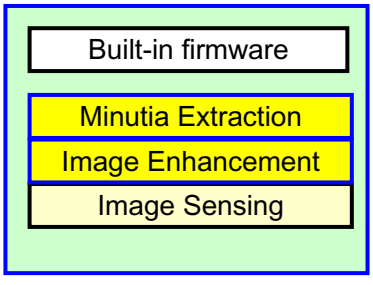


FP-RADAR BASE stores a template database and log files. Fingerprint images for templates are captured with our optical fingerprint register at the server.

Photo: Fingerprint register for sever / Model FP-200LSC

FP-Secure Gate Terminal

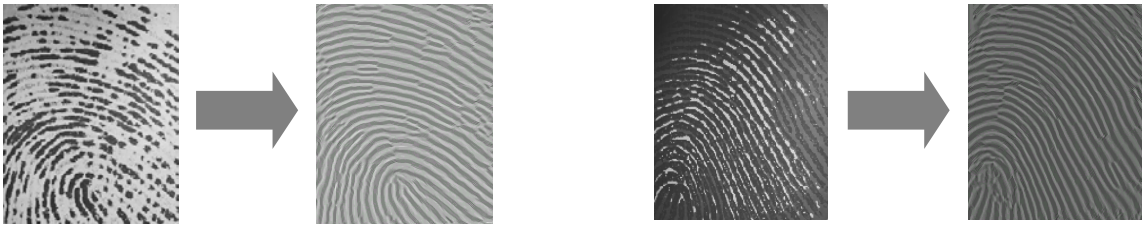
Photo: Gate terminal / Model FP-320



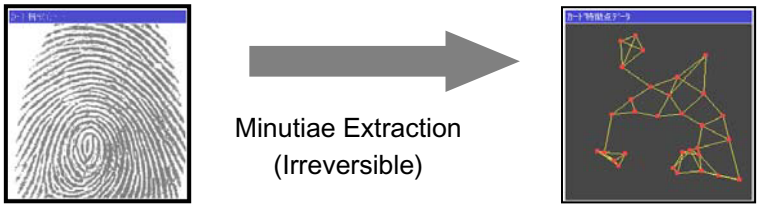
Functional Diagram of Gate Terminal

Additional Capability of FAST21

FAST21 has superior fingerprint image enhancement capability for reproducing desired contrast of an acquired fingerprint image.



FAST21 uses our unique minutiae extraction method for constructing a matching template. Processing time for generating a fingerprint template by **FP-Workstation** is approximately 0.24 msec per fingerprint image of the MST sample data set.



2. Component List and Cost Breakdown for System

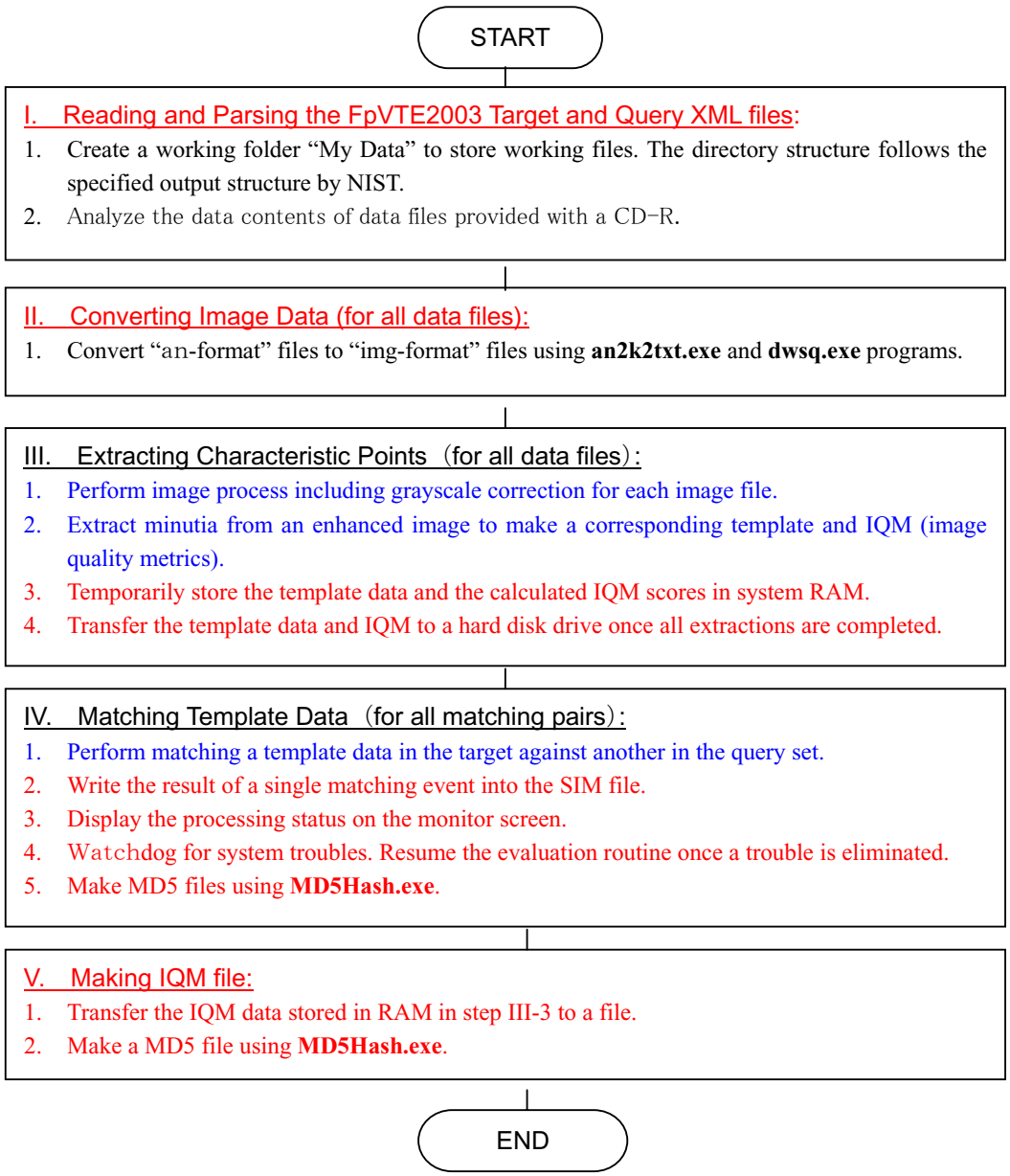
FP-Workstation has the following system configuration:

Item	Description	Qty	Cost (US $)
The	HP Workstation Model xw6000/CT with the following specification: Dual Xeon processors (3.06GHz/ 533MHz/ 1MB); 2GB 266 DDR RAM (4x512); NVIDIA Quadro4 299NVS; Dual Channel Ultra 320 SCSI 36GB, 15000 rpm; 48X IDE CD-ROM drive; 48x/24x/48X CD-RW Drive; 3.5” Floppy Disk Drive; PS/2 Scroll Mouse; MS Windows XP Professional.	1	6,141
2	View Sonic 19” LCD Monitor Model VX900	1	790
3	APS Uninterruptible Power Supply Model XS 1500 (1500VA)	1	250
4	Technoimagia **FAST-Verify** Library for Developer	1	10,000
5	Norton Antivirus Software (2004 version)	1	60

Remark: The processing speed of **FAST 21** is approximately proportional to the clock frequency of CPU you use. Items 1 may be replaced by a lower end PC to configure cost-effective **FP-Workstation**. Other than the processing speed, the output results and the accuracy are the same. For example, a single CPU (1.4GHz Pentium 4) based PC rerecorded matching speed approximately 11.8 msec per matching for the MST sample data set.

3. Customization for FpVTE2003

We have customized **FP-Workstation** for *FpVTE2003* according to the requirement of *FpVTE203*. In the flow chart shown below, steps in red were newly programmed for *FpVTE2003* whereas steps in blue are based on our tool library module, **FAST-Verify**.



***NOTE**: Programs "an2k2txt.exe" and "dwsq.exe" are part of NFIS (NIST Fingerprint Image Software). "MD5Hash.exe" is part of FpVTE 2003 Sample Utilities*

.

System Description Document

Overview

Ultra-Scan is a producer of fingerprint based identification systems. For eight years Ultra-Scan has manufactured ultrasonic (high frequency sound waves) based fingerprint readers which produce extremely high quality fingerprint images. By using high quality input images as input to our systems, we have been able to achieve a much higher level of overall system accuracy, as compared to competing systems.

Our mature match algorithms were developed in house by the same team of scientists and engineers who developed the original AFIS system installed in the FBI thirty years ago. The majority of our efforts have been focused on optimizing the algorithms using the high quality images produced from our ultrasonic fingerprint readers. **Please note, the image database used in the FpVTE 2003 Medium Scale Tests (MST) we participated in were collected using optical scanners, which do not produce the same high quality images as our ultrasonic based readers.** As such, we do not expect to achieve the same level of performance we would if using ultrasonic based fingerprint images.

Currently, Ultra-Scan offers three software products to our customers and partners:

1. IDExpress Developer, an SDK which allows a system integrator to incorporate our fingerprint match technology into their own application, creating their own GUIs for a unique “look & feel.”
2. IDExpress Enterprise, a complete, fully scalable and highly configurable and customizable AFIS built upon the IDExpress Developer foundation product listed above.
3. Independent Verification & Validation (IV&V), a software performance measurement and analysis routine and service which allows us to access the exact performance a particular system is achieving during any given time interval. It’s design provides for discreet and/or comparative performance measurement of BioAPI imaging devices and matching algorithms and provides the means of identifying sources of performance limitations and anomalies.

All three systems are built on the same underlying match technology. For FpVTE 2003, we choose to evaluate the IDExpress Developer and IV&V products, as IDExpress Enterprise does not support the unique requirements of the test without modifications.

Component list for the system(s) to be evaluated

IDExpress Developer
Off-the-shelf PC with standard Windows operating system
IDExpress Developer
Test Application using IDExpress Developer

IV&V
Off-the-shelf PC with standard Windows operating system
IV&V

Detailed cost breakdown of the submitted systems

IDExpress Developer
Cost is determined by application market, number of expected enrollees, and number of expected match attempts.

IV&V
Cost is determined by number of enrollees, number of inquiry match attempts, length of time to be analyzed, and detail of analyses to be performed.

Details of any modifications required to take FpVTE 2003

IDExpress Developer
IDExpress Developer is an SDK. An application was developed using IDExpress Developer specifically for the unique requirements of the FpVTE 2003 test.

IV&V
The unique requirements of FpVTE 2003 were incorporated into the standard product prior to testing; IV&V was used as an off-the-shelf package for the test.